

I want you to hear...

SANTA ANA FROM 4.926

Claudia Strauss

29 MAY 201

We need voting machines
that have a paper
trail and cannot
be hacked!

Sincerely,

Claudia Strauss

Please Act Now.

cardthartic.com

Claremont, CA 91711

RECEIVED JUN 04 2019

POSTCARD USA



TO

U.S. Election Assistance Commission
1335 East West Highway
Suite 4300
Silver Spring, MD 20910

20910-322599



PLEASE
LISTEN

I want you to hear...

PLEASE BE DILIGENT IN 2020
PROTECTING OUR ELECTIONS
FROM FOREIGN INTERFERENCE. OUR COUNTRY IS
UNDER ATTACK BECAUSE
OF PAST SUCCESSES.

THANKS

Donald Martens

Please Act Now.

SANTA ANA, CA 926

DONALD MARTENS

POMONA, CA. 91767

POSTCARD USA

cardthartic.com

RECEIVED JUN 04 2019

TO COMMISSION

U.S. ELECTION ASSISTANCE

1335 E. WEST HIGHWAY
SUITE 4300

SILVER SPRING, MD
20910

PLEASE
LISTEN

I want you to hear...

DEAR SIR/MADAM -

SANTA ANA CA 926

FROM

MEG MATTHEWS

30 MAY 20

WE KNOW THAT RUSSIA
INTERFERED WITH THE 2016
ELECTION + IS ATTEMPTING
TO DO THE SAME IN 2020.
WE MUST PROTECT THE INTEGRITY
OF OUR ELECTIONS — THE
BASIS OF OUR DEMOCRACY.

PLEASE PROTECT US BY
PROHIBITING VOTING SYSTEMS
FROM CONNECTING TO THE
INTERNET. WE NEED CLEAR
FIREWALLS SO **Please Act Now.**
OUR VOTES WILL

BEING COMPROMISED.

THANK YOU! — MEG MATTHEWS.

POSTCARDUSA

CALIFORNIA, CA 91711

TO

RECEIVED JUN 04 2019
U.S. Election Assistance Commission

1335 East West Highway
Suite 4300

Silver Spring, MD

20910

PLEASE
LISTEN

**U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910**

Charles Gregory

[REDACTED]
Albuquerque, NM 87123

June 3, 2019

Dear EAC:

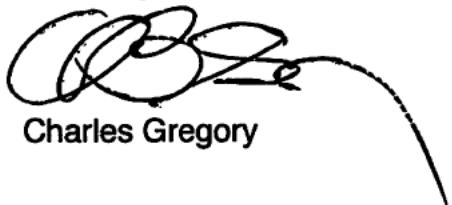
I am increasingly distrustful of the integrity and reliability of our democratic vote.

Specifically, as it relates to the commission, I am dubious we are capable of preventing the manipulation of our electronic voting machines — and not just by the Russians.

I'm given to understand one of the easiest ways to hack our electronic machines is to have them connected to the public internet.

I'd be happy if we jettisoned electronic voting machines altogether, but that's not likely to happen. So you really need to do all you can to protect them from manipulation. Eliminating the public internet is a good start. I'm sure there's much more.

Sincerely



Charles Gregory

Men~~talmen~~
RECEIVED JUN 04 2019

Please ensure Voting Systems by prohibiting
Voting machines from connecting to the Internet
or Cell networks.

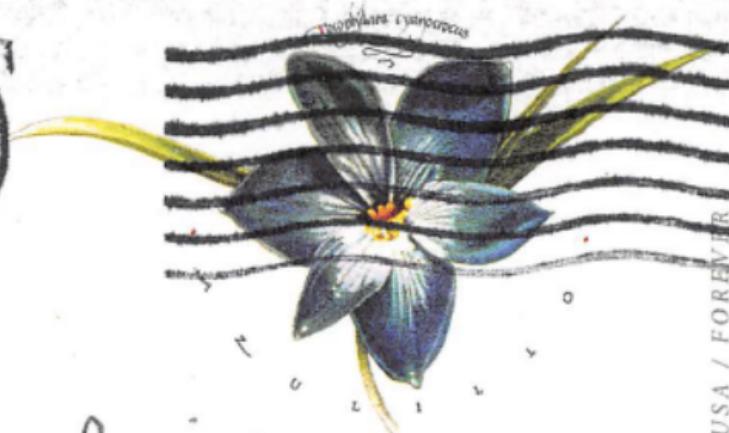
- The US is still dealing with the fallout of
the Russian interference in the 2016 election.

- Both the FBI and the Dept. of Homeland
Security have confirmed all 50 states election
Networks have been targeted
attacks.

new
Vote Centers

Reyes

[REDACTED]
Walnut, CA 91789



USA / FOREVER

US Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

**Before the
U.S. ELECTION ASSISTANCE COMMISSION**

In the Matter of) COMMENTS SUBMISSION
VOLUNTARY VOTING SYSTEM) Pursuant to 84 FR 6775, Doc. No.: 2019-03453
GUIDELINES VERSION 2.0) Wednesday, May 29th, 2019
DEVELOPMENT) EAC Offices, Silver Spring, MD

PUBLIC COMMENTS SUBMISSION

OSET INSTITUTE COMMENTS LED BY GLOBAL DIRECTOR OF TECHNOLOGY EDWARD P. PEREZ
REGARDING
THE VOLUNTARY VOTING SYSTEM GUIDELINES VERSION 2.0 PRINCIPLES AND GUIDELINES

Comment #1

Issue: Principles and Guidelines vs. Functional Requirements

Reference: Overall VVSG 2.0 Structure

The OSET Institute applauds the U.S. Election Assistance Commission (hereinafter, “EAC”) for making efforts to ensure that the future *Voluntary Voting System Guidelines* (VVSG) certification program is more flexible and agile than it has been in the past. With increasingly faster advances of technology matched by newly emerging cyber-security threats, it is essential for the VVSG to support regular adaptation and modification. Toward that end, VVSG 2.0's initial distinction between "*Principles and Guidelines*" versus "*Functional Requirements*" is well placed and laudable. In order to deliver on the promise of such a distinction, the OSET Institute believes that the following programmatic requirements must be adhered to:

- “Principles and Guidelines” reflect policy statements, and any modifications to the *Principles and Guidelines* should require approval of EAC Commissioners.
- Functional Requirements (and VSTL test assertions) do *not* represent policy statements, and their modification should *not* require approval of EAC Commissioners. Functional Requirements are simply the technical means to *operationalize* or *implement* the achievement of policy goals represented in the *Principles and Guidelines*.
- Functional Requirements must support the policy goals represented in the *Principles and Guidelines*.

- The OSET Institute's position on the above assertions is in agreement with the *National Association of State Election Directors* (NASED) and the *Center for Democracy and Technology* (CDT). Without these important programmatic distinctions between modifications of Principles vs. modifications of Requirements, the danger is that the VVSG 2.0 certification program will simply re-create the cumbersome scope, complexity, and dependencies that have led to relative inertia in the voting technology marketplace. This inertia has not served the needs of Election Officials or U.S. national security.
- The OSET Institute believes that the programmatic distinctions recommended above are entirely consistent with the EAC's own statement of "*Roles and Responsibilities Of the Commissioners and Executive Director of the U.S. Election Assistance Commission*" (<https://www.eac.gov/assets/1/1/EAC%20Roles%20and%20Responsibilities.pdf>):

*Issuance of Policy Directives: A policy directive is a document, which states agency **goals and objectives** or sets the **scope** of an EAC program. It is a means by which the commissioners may make a policy statement or determination in any area of EAC operations. A policy directive is a **short, simple document** that informs staff of the **high-level goals or objectives** for a particular EAC program or operation. This tool provides the commissioners with a means to set and document policy in a transparent way, which provides clear guidance to **implementing** staff. [Emphasis added]*

- None of the characteristics of policy could reasonably be said to apply to the Functional Requirements. They do not describe goals or objectives; they do not set the scope of the certification program; and their specifications are most certainly not "short," or "simple." However, Functional Requirements are a means to *implement* policy goals.
- If and when the VVSG 2.0 *Principles and Guidelines* are initially voted upon by the Commissioners, the *initial* set of Functional Requirements associated with VVSG 2.0 *Principles and Guidelines* should also be voted upon at the same time, as part of the overall initial "package." (Note: The OSET Institute believes that Test Assertions for voting system test laboratories should be excluded from the initial "package" to be voted upon, and should never be required to be put to a vote.)
- After the adoption of initial VVSG 2.0 *Principles and Guidelines* and Functional Requirements, the EAC should devise a process by which future modifications and/or re-interpretation of functional requirements can be administered based upon a joint voting process that includes the *Technical Guidelines Development Committee* (TGDC), the *EAC Standards Board*, and staff of the EAC Testing and Certification Program. The current process for *Requests for Interpretation* (RFI) of VVSG requirements might serve as a useful starting point for how changes could be considered and promulgated, provided that the TGDC and Standards Board have opportunities to provide feedback and to vote on new interpretations or new requirements.

- It should be emphasized that the OSET Institute does *not* believe that Functional Requirements should be capable of being officially changed *solely* by the staff of the EAC Testing and Certification Program. Furthermore, the OSET Institute also recommends that any time the TGDC, Standards Board, and staff are considering a change to Functional Requirements, input should also be solicited from EAC-accredited voting system test laboratories (VSTLs).
- The OSET Institute recommends that, as part of the process by which the TGDC, Standards Board, and EAC staff consider changes to Functional Requirements, a process mechanism must *also* be put in place by which the joint body may vote to require consultation and approval from the Commissioners on selected requirement changes, in exceptional cases that are deemed to be particularly sensitive or consequential.
- The authority to change the VVSG Principles and Guidelines or to introduce new ones preserves the EAC Commissioners' essential role, notwithstanding the programmatic recommendations described above. Any time the EAC Commissioners fulfill their duty to promulgate important policy statements through the *Principles and Guidelines*, such will lead to cascading Functional Requirements for voting system technology, to meet newly-prioritized policy goals, and thereby impacting future voting technology development. The importance of this role should not be underestimated.
- The OSET Institute believes that none of the recommended procedures above contravene the continuance of robust Roles and Responsibilities for EAC Commissioners. Indeed, the EAC's "*Roles and Responsibilities*" document outlines important ongoing duties for Commissioners, including matters of strategic planning and agency objectives:
<https://www.eac.gov/assets/1/1/EAC%20Roles%20and%20Responsibilities.pdf>

Comment #2

Issue: Lack of Glossary

Reference: Overall VVSG 2.0 Structure

The 9.12.2017 version of the VVSG 2.0 *Principles and Guidelines* currently published on the EAC web site regarding the Public Comment Period lacks a Glossary. The OSET Institute recommends that prior to official adoption, the VVSG 2.0 *Principles and Guidelines* should formally incorporate a glossary that is also available for public review and comment.

The OSET Institute *strongly* encourages that the VVSG 2.0 *not* "re-use" or "copy-and-paste" the existing glossary in VVSG 1.1. Precise definitions and re-assessment of essential terms are a critical part of securing the foundations of the VVSG 2.0 certification program.

Comment #3

Issue: Lack of definition of “voting system”

Reference: Overall VVSG 2.0 Structure

The VVSG 2.0 *Principles and Guidelines* frequently use the term “voting system,” although this phrase is not defined (see also *Comment #2, supra*). The OSET Institute *strongly* recommends that the EAC’s past understanding of “voting system” be re-assessed and modified to provide more flexibility and agility in the future.

The *Help America Vote Act of 2002* adopted a broad definition of “voting system” for *legislative* purposes, encompassing a total combination of a wide scope of components, functions, practices, and documentation in its description of the term. The OSET Institute believes, however, that that *legislative* definition was needlessly implemented by the EAC as an erroneous *programmatic* requirement that the EAC will *test and certify* only entire “total” system configurations. Notwithstanding typical practices from major voting system vendors and testing authorities in recent decades, we believe that the EAC has an important opportunity to consider the scope of “systems” and “components” to which the VVSG 2.0 requirements are applicable in a more flexible and nuanced way.

More specifically, the OSET Institute recognizes that although past certification campaigns have been focused on “total” system configurations that include a comprehensive minimum set of end-to-end functions, there are alternative ways of defining a “voting system” in a manner that could still be consistent with HAVA’s definition. It is the OSET Institute’s view that few things have been more consequential for innovation and choice, or the lack thereof, than an exclusively “totalizing” conception of a voting system. The assumption that any manufacturer of a “voting system” to be certified must be able to provide *all* components that could potentially fall with HAVA’s broad description of a “voting system” has vastly increased the complexity of development, deployment, and support. As a result, the implementation of this broad HAVA definition, while likely a well-intentioned effort to “leave no stone unturned,” has ironically resulted in a highly-concentrated marketplace that reduces competition, increases dependence on vendors, and leaves our nation’s elections officials with more limited choices.

The growing concentration in the voting technology industry, where the two largest providers supply voting systems for approximately 80% of the nation’s registered voters, coupled with the fact that only *one* new vendor has meaningfully entered the marketplace in the past decade, dramatically illustrates how complexity can produce inertia. An exclusively “total” conception of voting systems means that the voting technology services market is effectively closed to broad range of government IT service providers.

In order to provide voting systems services and support to the U.S. market, a company must first pay the up-front cost and ongoing costs of developing, certifying, and delivering a proprietary voting system product to customers, along with the services and support contracts that go along with the products. Furthermore, even considering EAC programmatic distinctions between “new” and “modified” systems, the re-certification process for updated voting equipment can be lengthy and expensive if a “voting system” is defined only in a broad, comprehensive way. These conditions can serve as a deterrent to

manufacturers making even minor updates. When the “hurdle” to be overcome is certification of an entire system, even to satisfy the need for merely small changes, voting system manufacturers perceive a limited return on investment in addressing the ongoing needs of current customers through value-added enhancements; instead, they focus on making functional changes to their systems mainly or even exclusively to open new regional markets, often leaving prior releases to lie fallow. This, in turn, can leave election officials more dependent on vendors, waiting for years for their preferred enhancements, and increasing the likelihood that voting technology development is “frozen.”

Comment #4

Issue: Transition to new VVSG 2.0 standards

Reference: Overall VVSG 2.0 Structure

The OSET Institute shares the EAC’s concern that no voting system manufacturer has submitted a system for testing to anything other than the 14-year old VVSG 1.0 standard; those 2005 requirements are not adequate for the current global environment, or for current voter needs. Accordingly, the EAC should implement policies that create incentives and/or requirements for manufacturers to develop systems designed to comply with newer standards. However, “blunt force” requirements that “sunset” prior standards too aggressively could pose challenges for state and local officials using older systems, by potentially disrupting continued support of deployed voting systems.

To achieve the right balance between these needs, the OSET Institute believes that the EAC *must establish a new policy that more clearly and precisely establishes a distinction between “new” versus “modified” systems.* As the Commission is undoubtedly aware, the EAC currently promulgates an “implementation period” each time a new VVSG standard is adopted, which transparently allows a transition period (typically 18 months) during which the EAC will accept submissions for testing and certification of voting systems to either the old standard, or the new standard; manufacturers get to choose. Under current practice, once the implementation period is over, the EAC is *supposed* to accept submissions for new systems *only* under the newer standard. However, the problem is that under current practice, the EAC *also* allows vendors to submit modifications to voting systems previously certified (i.e., under the VVSG 1.0 standard), *without ever having clearly established what constitutes a “new” system versus a “modified” system.* The EAC *Testing and Certification Program Manual* includes only a *formal* definition of “new” vs. “modified,” and not a substantive one (i.e., a “new” system is a system not previously certified, and a “modified” one includes changes to a system previously certified). Needless to say, this open-ended “definition” is not particularly helpful in knowing when to forestall further “modifications.”

To be clear: The OSET Institute believes that it is critically important to allow manufacturers to continue supporting deployed legacy systems under older standards for a *reasonable* amount of time. But 14 years after the adoption of VVSG 1.0 is not a “reasonable” amount of time, and manufacturers are currently taking advantage of a lack of clarity in EAC Program Requirements and EAC policy.

Under the EAC's prior *Director of Testing and Certification*, pinning down manufacturers on whether they were submitting a "new" versus a "modified" system for certification became a torturous exercise in hair-splitting semantics because, surprisingly, the EAC tried to make it an official policy to allow manufacturers to determine *for themselves* what constitutes a "new" versus a "modified" system, by simply telling manufacturers that they need to define these classifications *for themselves* and document them in their own configuration management and version control policy manuals ([https://www.eac.gov/assets/1/6/NOC_17.01_NewSystem\(FINAL\)7.18.17.pdf](https://www.eac.gov/assets/1/6/NOC_17.01_NewSystem(FINAL)7.18.17.pdf)).

This has not worked well, as it has led to confusion, uncertainty, and legalistic squabbling back-and-forth between manufacturers and the EAC. All of this gamesmanship has ultimately allowed the manufacturers to keep submitting modifications under the VVSG 1.0 standard, with no discernible end in sight. (Indeed, several manufacturers insist that they have no intention of developing systems to the March 2015 VVSG 1.1, and they indicate they will wait until VVSG 2.0 is finalized before developing *anything* to a newer standard – which makes it likely that many "new" voting systems used in 2024 will be based *on a 20-year old standard*.)

The Institute believes this situation *must* be corrected. Until manufacturers face more comprehensive restrictions on their ability to make modifications to currently certified systems under old VVSG standards, they will probably continue to do so. Accordingly, the OSET Institute recommends:

1. The EAC must devise a precise, substantive policy statement on the difference between a "new" versus a "modified" voting system.
2. The EAC should consider setting an "expiration" time window that would be associated with any new voting system's eligibility to be tested for compliance with the standard to which it is originally tested. For example, after the first submission of a "new" voting system to any particular standard, the EAC could impose a five-year limit on that system's eligibility to test for compliance with the same standard, *assuming a newer standard is available*. Based on past history, the time required for manufacturers to develop, test, and certify a voting system to new standards is approximately five years, and this time window would allow adequate time for manufacturers to develop a product roadmap in anticipation of any new requirements, and it would encourage them to make sure that their roadmap simultaneously provides for support of older systems, while also preventing them from avoiding new standards indefinitely, and (at least gently) forcing them to move forward, and develop toward the future. Even during the long period from 2009 to 2015 when the EAC lacked commissioners to adopt VVSG 1.1, the vast majority of its substantive content was available to the manufacturers, and there was only modest risk in developing new products to those draft requirements.
3. In concert with recommendation #2, *supra*, the EAC must ensure that any new definition of a "modified" system allows manufacturers to continue support of older deployed systems in a predictable way, to avoid the costly, disruptive, and painful unintended consequence of potentially "freezing" important and potentially necessary changes to voting technology platforms that state and local election officials might have just purchased.

4. The EAC should *disallow* manufacturers from “re-classifying” a previously certified, previously modified system as “new,” simply to “restart” the clock for further modifications under an older standard, thereby extending the life of old platforms in perpetuity.
5. As described in [Comment #5, infra](#), the EAC should implement a *component-level* certification program, which would greatly mitigate many of these potential “bottlenecks” in the voting technology marketplace.

Comment #5

Issue: Certification of modular components

Reference: Overall VVSG 2.0 Structure

In contrast to the unintended consequences of testing voting system components only as full systems, and in light of upcoming revisions to the EAC *Testing and Certification Program Manual* associated with VVSG 2.0, the OSET Institute believes that new procedures for testing could be an enabler for positive market transformations. Specifically, component-level certification, in conjunction with VVSG 2.0 requirements to support *NIST Common Data Formats*, could introduce greater diversity and agility in the voting system marketplace – both of which are essential in a rapidly changing threat environment.

By “component-level certification,” we mean the ability for manufacturers to develop, test and seek certification for individual portions of a voting system, rather than being required to submit only entire systems for certification. This approach has the potential for a more diverse group of technology providers to develop systems in accordance with their greatest strengths, and it also allows finer distinctions between mission-critical voting components (e.g., device configuration, vote casting and vote capture), versus less security-centric applications (e.g., election data management and ballot design). Ballot design tools might benefit, for example, from being developed by providers with graphical design and usability testing skills that are quite distinct from the skills needed to produce secure single-function voting devices.

An approach based on component-level certification and interoperability through VVSG-required support for Common Data Formats has the further benefit of being advantageous to traditional voting system manufacturers and new market entrants alike. With this approach, traditional vendors could continue developing and submitting for certification entire comprehensive systems, as they do today; or they could be even more responsive to individual customer needs, by making only component-level changes and submitting individual components for certification, accordingly; and new vendors who do not wish to develop entire voting systems could also enter the marketplace, based upon their fields of expertise.

Based on current federal certification practices, many states already regularly seek their own flexible approaches to certification, and they are likely to continue to do so, regardless of what does or does not change under the VVSG 2.0 program. For example, some states have abandoned federal certification

requirements altogether, and some have chosen to effectively do their own component-level testing.¹ However, if the federal certification process were to introduce a similar level of flexibility, this would allow new technology developments to become beneficial to jurisdictions across the country, rather than being localized to only certain states. In this way, the EAC certification could thereby “raise the bar” for the overall state of the art, by allowing wider distribution and deployment of technology innovations.

In sum, with component-level certification, open data standards and a different conception of “voting system,” a broader range of IT service providers would be able to compete for government contracts for voting system integration, deployment, services, and support – with reduced emphasis on monolithic proprietary voting system products. This would then be an enabler for market transformation, in which election officials would have more choices for election technology and service providers (with potentially lower prices, as well, due to the possibility of less one-sided contracting terms).

Furthermore, because so much thoughtful effort has already been put into VVSG 2.0 Functional Requirements, due to more than a decades’ work of engagement and learning by many stakeholders, much of the effort that would be required to devise standards for individual voting system components has already been done. There is also emerging consensus on the most mission-critical components, including ballot scanners, tabulation software, and voting device configuration tools.

At a recent Public Hearing in Memphis, Tennessee, [EAC Commissioner Donald Palmer](#) asked, “*What might a component-level certification program look like? How might it work?*” The OSET Institute respectfully submits these considerations as *starting points* for a new framework for component-level certification; needless to say, much additional work remains to be done in devising the details of such a program:

1. Before the VVSG 2.0 Functional Requirements are finalized, they should be reviewed to make the presentation of requirements as “modular” as possible, so that “families” of requirements can be clearly and explicitly associated with specific types of voting system components. This should not be difficult, as this way of “grouping” requirements is already consistent with past practice. For example, past versions of the VVSG have identified requirements for “*Election Management Systems*,” “*Accessible Voting Stations*,” “*Precinct Count*,” “*Central Count*,” and “*Vote Tabulating Program*.” Furthermore, current draft VVSG 2.0 requirements (as discussed in the Public Working Groups) *also* appear to naturally “group” many requirements in association with particular functional components. Accordingly, it should be possible to draw a “bright line” or “boundary” around the requirements associated with each type of voting system component, by simply extracting and consolidating relevant requirements from the Functional Requirements, as currently drafted.

¹ Examples of state and local efforts to introduce greater flexibility in the development and certification process include the *California Voting System Standards* (October 2014); Washington’s *Election Modernization Project*; and Los Angeles County’s *Voting Solutions for All People* (VSAP) project.

2. Assume that each type of component must support all applicable requirements traditionally enumerated in VVSG “Overall System Capabilities” (e.g., security, accuracy, error recovery, integrity, audit logging, etc.). The “overall capabilities” have traditionally been “uniform” requirements that encompass high-level best practices and design features that would be desirable in all components, whether it is an EMS software application, a ballot marking device, or a central count scanner, for example.
3. In addition to specifying a consolidated set of requirements that applies to specific modular components of the voting system, for each type of modular component, EAC staff and VSTLs must also identify additional dependencies for each type of voting component, particularly with an eye toward the three “classic” categories of overall system workflow, namely: pre-voting, voting, and post-voting. So, for example, if a manufacturer submitted for certification only a precinct scanning voting device, there would certainly be dependencies between that device and the post-voting tabulation program; and the format in which the scanning device creates Cast Vote Records, for example, would need to be consistent with post-voting tabulation requirements for certain types of reporting or cryptographic validation, for example. By “mapping” “families of requirements” associated with different types of voting components to *other* system components where dependencies exist, a fuller picture of the requirements can be built, and those associations would also inform protocols for integration testing.
4. All voting system components should be required to support the import and export of data in an interoperable format that complies with the NIST 1500-100 Common Data Format (CDF) specification (again, for different categories of the election (i.e., pre-voting; voting; and post-voting)).
5. When manufacturers of voting technology apply for EAC certification, they would have the *option* of submitting a configuration that is *either* a) a complete voting system configuration; or b) one or more individual components only. Consistent with current practice, each manufacturer’s Implementation Statement would indicate which functions and capabilities the component(s) or system are intended to support.
6. Consistent with current practice, EAC-accredited VSTLs would make an overall assessment of which VVSG Functional Requirements are applicable to the system or components, or, alternatively which requirements are not applicable, and thus excluded from the scope of testing. These determinations would be described in the Test Plan for any submitted component or configuration.
7. For manufacturers that are submitting one or more components that are compatible with previous EAC-certified systems, it is a virtual certainty that those manufacturers would have performed their own internal integration testing to assure end-to-end compatibility with other system components, and the results of that testing would be documented. In such instances, the EAC should require manufacturers to submit appropriate Attestations, detailed test modules, and test results to demonstrate integration performance with other known systems or components.

Those test results would be a supplement to additional testing by VSTLs, to ensure that the submitted components support the NIST Common Data Format for interoperability.

8. The use case that is genuinely new territory and that will require additional specification in any revised certification program is as follows:

A non-traditional manufacturer wishes to submit only one component for certification, and a specific use case for integration testing with another specific system has not yet emerged.

- a. Suppose, for example, that a new market entrant submits a ballot layout software application that can import and export data in the NIST CDF. Further, suppose that at the time of application for certification, the manufacturer has not yet identified a specific buyer that wishes to use the software application in conjunction with another vendor's named voting devices.
- b. In such a use case, VSTLs would need to devise robust protocols and mock elections to ensure true interoperability based on the NIST CDF. On the other hand, it is often the case that the "driver" for a federal certification campaign is a voting technology procurement for a specific state or jurisdiction, or it is a market entry into a specific region of the country.
- c. In such instances, likely configurations may be known, or another vendor's system required for integration will already have been identified.
- d. Furthermore, specific state requirements in such instances are likely to be important inputs to the federal certification process, and collaboration regarding integration would likely be easier to accomplish (i.e., between states, EAC staff, VSTLs and manufacturers).
- e. In such cases, the "unknowns" would be reduced, and the path to true integration testing might be easier to identify.

Comment #6

Issue: Cybersecurity

References: Principles 11, 12, 13, 14, and 15

The OSET Institute respectfully submits that the EAC is in dire need of elevated cybersecurity expertise – both in quality and quantity. Cybersecurity to protect our national sovereignty against cyber-warfare attacks from foreign nation-state actors is not currently one of the core competencies of the EAC, nor of the EAC's accredited Voting System Test Laboratories (VSTLs). Robust cybersecurity resources will be necessary to ensure the implementation of security-related principles 11, 12, 13, 14, and 15. The OSET Institute believes that the EAC should avail itself of such resources from the Department of Homeland Security (DHS), which *does* have core competencies in high-assurance computing and cybersecurity.

Comment #7

Issue: Penetration testing

References: Principles 11, 12, 13, 14, and 15

The VVSG 2.0 *Principles and Guidelines* do not currently have explicit requirements for voting systems to undergo penetration testing by accredited third-party testers, and current VVSG standards (1.0 and 1.1) also lack such requirements. Penetration testing (which is outside the core competencies of current EAC VSTLs) should be a mandatory part of the VVSG 2.0 testing and certification program.

Comment #8

Issue: Documentation

References: Principle 3.1

Current Principle 3.1

The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

The OSET Institute believes that the principle above is simply under-determined. It is so abstract as to be almost meaningless, as it does not specify answers to even basic questions such as, “*readable and understandable by whom?*” Is that intended to be EAC technical examiners, trained engineers, election staff, poll workers, or even voters? Accordingly, we recommend the changes below.

Recommended substitute language, Principle 3.1

The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system shall be written in sufficient detail and style to be capable of being read and understood by the end-user audience that will interact with the applicable voting system component(s).

Comment #9

Issue: Distinction between capabilities of voting system, versus capabilities of users

References: Principle 3.3, 5.1, 5.2, 6.2, 7.2, 7.3

As currently written, most of the *Principles and Guidelines* correctly describe functions or capabilities that voting systems must support; in other words, the focus is correctly placed on what is required of the technology system. However, in several instances the *Principles* veer off-course, by using language that describes what is required or expected of *users*, or *voters*, instead of the voting system. Substitute language should be employed to describe the capabilities that are required *of the voting system*.

Examples

Current Principle 3.3

The public can understand and verify the operations of the voting system throughout the entirety of the election.

Recommended substitute language, Principle 3.3

The voting system includes features that support the ability of election officials, examiners, auditors, voters and other stakeholders to understand and verify the operations of the voting system throughout the entirety of the election.

Current Principle 5.1

Voters have a consistent experience throughout the voting process in all modes of voting.

Recommended substitute language, Principle 5.1

The voting system includes features that facilitate a consistent experience across each individual voting session, throughout the process, in all modes of voting.

Current Principle 5.2

Voters receive equivalent information and options in all modes of voting

Recommended substitute language, Principle 5.2

The voting system provides equivalent information to each individual voter, across all modes of voting, in accordance with each voter's chosen modality.

Current Principle 6.2

Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others

Recommended substitute language, Principle 6.2

The voting system supports all voters' ability to mark, verify and cast their ballots without assistance from others.

Current Principle 7.2

Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

Recommended substitute language, Principle 7.2

The voting system includes features that facilitate voters' and election workers' accurate use of controls, in the manner that voters and election workers intend; and

The voting system includes features that provide voters with direct control of changes to ballot presentation and voter selections.

Current Principle 7.3

Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Recommended substitute language, Principle 7.3

The voting system includes usable features that facilitate a voter's ability to understand all information as it is presented, including informational and error messages from the system.

Comment #11

Issue: Interoperability

Reference: Principle 4.1

Principle 4.1 should explicitly state, “*Voting system data that is imported, exported, or otherwise reported, is in an interoperable format that complies with the NIST Common Data Format specification.*”

Comment #12

Issue: Consistent voting experience

References: Principles 5.1 and 5.2

The hazard exists that Principles 5.1 and 5.2 could be read/interpreted to mean that all voters must have exactly the same voting experience, i.e. if some voters are using certain types of equipment, modes of voting, or specific features, then any deviation from those would constitute an “inconsistency” that violates the principle. But this should not be the case, as there are, for example, many instances when voters use different modalities that result in different experiences. Some voters might use a remote accessible vote-by-mail system, which employs an electronic interface at home, and others might hand-mark an absentee or precinct ballot, and still others might use an accessible ballot marking device in a polling place. Within the same election at the same jurisdiction, it should be possible for *all* of these voting methods to be employed, without violating the principle, so long as each voter’s experience ***within their own chosen mode of voting*** is consistent. (For example, if a voter is using an electronic interface at home with large type, then ballot instructions should also be available in large type.)

As noted in [Comment #9 supra](#), the OSET Institute recommends the following substitute language for Principles 5.1 and 5.2:

Current Principle 5.1

Voters have a consistent experience throughout the voting process in all modes of voting.

Recommended substitute language, Principle 5.1

The voting system includes features that facilitate a consistent experience across each individual voting session, throughout the process, in all modes of voting.

Current Principle 5.2

Voters receive equivalent information and options in all modes of voting

Recommended substitute language, Principle 5.2

The voting system provides equivalent information to each individual voter, across all modes of voting, in accordance with each voter's chosen modality.

Comment #13

Issue: Voting without assistance

Reference: Principle 6.2

It should be noted that the laudable high-level goal of allowing all voters to 1) mark; 2) review; 3) verify; and 4) cast their ballots “*without assistance*,” as well as related VVSG requirements to allow such activities “*without manually handling the ballot*” might lead to some complex, costly, and potentially insecure outcomes. The EAC’s prior *Director of Testing and Certification*, for example, interpreted VVSG 1.1, Sec. 3.3.4(b)² to mean that *only* and *exclusively* an “all-in-one” ballot marking—verifying—scanning device could possibly comply with requirements for accessible paper ballot voting. *Anything* that required more than one device was regarded as non-compliant.

What is left unsaid in such interpretations, or in VVSG 2.0 Principle 6.2, however, is that most computer science and engineering experts regard such “all-in-one” device designs as being notoriously insecure. *Why?* Fundamentally, it is problematic to locate end-to-end voting functions on a single voting device, because it creates the opportunity for a malicious actor to tamper with a single device to manipulate the entire voting process. (In contrast, for the very same reasons, until very recently, most in the election community *insisted* that “ballot verification stations” must be *independent* of all marking and/or scanning capabilities.) It appears to be only in light of more recent concerns about “no manual handling” that visions of “all-in-one” devices appear on the rise, at least implicitly (if not explicitly).

² “The Accessible Voting Station shall provide features that enable voters who lack fine motor control or the use of their hands to submit their ballots privately and independently without manually handling the ballot”; similar functional requirements exist in draft VVSG 2.0.



As outlined by computer science professor [Andrew Appel](#) of Princeton University (who served on the National Academies of Science, Engineering and Medicine’s “*Committee on the Future of Voting*”) the problem with all such designs is that they makes it possible for the voting device to potentially print more votes on a voter’s ballot, even after the voter has reviewed and verified it, because the “all-in-one device” has a single paper path, from marking to printing to casting. As a result, the marked ballot that the voter reviews and verifies might not be the same ballot that is seen by an auditing or recount team, for example. (See, for example, <https://freedom-to-tinker.com/2019/03/08/reexamination-of-an-all-in-one-voting-machine/>)

Finally, it should also be noted that any interpretation of Principle 6.2 as necessarily requiring an “all-in-one” design with a non-manual paper transport mechanism would immediately render obsolete virtually every EAC-certified design that currently exists for accessible paper ballot marking. What used to be acceptable paper ballot marking device platforms could be rendered non-compliant for future configurations, virtually overnight, thereby “dead-ending” deployed devices for future upgrades (which, needless to say, has an adverse impact on state and local election officials), and it would also require state and local officials to acquire costly *new* accessible devices in the future (only after manufacturers design such devices, also at considerable cost).

The OSET Institute points out this concern with Principle 6.2 to caution that its implementation would be problematic if it is interpreted as exclusively allowing “all-in-one” voting device designs to be compliant. As always, there must be a balance between security and accessibility.

Comment #14

Issue: Default voting system settings for ballot display

Reference: Principle 7.1

Current Principle 7.1

The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs

The OSET Institute believes that the phrase “widest range of voters” is under-determined, and we cannot imagine a testable way of specifying such a thing.

Comment #15

Issue: Usability and accessibility

Reference: Principle 8.3

Principle 8.3 should state, “*The usability and accessibility of a voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.*”

Comment #16

Issue: Usability by election workers

Reference: Principle 8.4

Principle 8.4 would benefit from more precise specification of the term “election workers.” At least two categories of “election workers” interact with voting system technology:

1. “Back-office” election staff that use Election Management System (EMS) software applications and/or voting devices; and
2. Poll workers that use polling place devices.

VVSG 1.1 currently requires usability testing for poll workers; it does not require usability testing for back-office election staff. Principle 8.4 should clarify what type of usability testing is envisioned.

The OSET Institute notes that usability testing for poll workers is well understood, and can be specified efficiently in a usability-testing plan. In contrast, meaningful usability testing with election office staff, for EMS applications, would likely be more complex, as such systems typically encompass many more features, options, and potential workflows in comparison to polling place operations.

Comment #17

Issue: Voter privacy

Reference: Principle 10

Principle 10 should state, “*VOTER PRIVACY. The voting system protects the privacy of voters.*”

The Institute believes “Ballot secrecy” is not an appropriate term-phrase. Ballot selections might be publicly viewable in a post-election audit, for example. The point, however, is to protect a voter’s *privacy*, by never allowing a voter’s ballot choices to be directly associated with an individual voter’s identity.

Comment #18

Issue: Physical security

Reference: Principle 12.2

Current Principle 12.2

The voting system only exposes physical ports and access points that are essential to voting operations.

Recommended substitute language, Principle 12.2

The voting system includes features to protect access to physical ports and access points; and

The voting system includes features to disable physical ports and access ports that are not essential to voting operations.



Verified Voting.org

Public Comments on VVSG 2.0 Principles and Guidelines

Submitted May 29, 2019

Verified Voting is pleased to see the VVSG 2.0 principles and guidelines finally moving forward. We are enthusiastic about the VVSG 2.0 structure and, with some reservations, about the content of the principles and guidelines. Full implementation of the VVSG 2.0 will, in time, help bring about voting systems that set new standards for universal usability, security, and verifiability. All these properties – backed by sound procedures – are essential to enable officials to run resilient elections, and to reassure voters that their votes have been cast as intended and counted as cast.

We urge the EAC to allow the technical requirements and test assertions to be approved and revised without a vote of the commissioners. We agree with the TGDC, the NASED executive council, and others that for several reasons, these documents are best managed by technical staff, adhering to a well-defined process with broad consultation and opportunity for public comment.

Verification and the VVSG

Verified Voting especially welcomes Principle 9, which stipulates that a voting system “is auditable and enables evidence-based elections,” and the associated guidelines. No matter how otherwise usable and reliable a voting system may be, it is unacceptably dangerous if it cannot provide trustworthy, software-independent evidence that people’s votes have been accurately recorded and counted.

A voting system alone can “enable” evidence-based elections but cannot provide them. As Philip Stark and David Wagner wrote in their seminal paper, the basic equation is that “evidence = auditability + auditing.” A voting system with a voter-verifiable audit trail, such as a voter-marked paper ballot, provides auditability. Compliance audits to ensure that the audit trail is substantially complete and accurate, and risk-limiting tabulation audits of the audit trail, provide actual evidence that outcomes are correct.

These considerations point to two ongoing challenges for the EAC and everyone else who works with the VVSG. One challenge is to communicate

that, in practice, voting system security largely depends on election procedures and especially on post-election audit procedures. Compliance and risk-limiting tabulation audits happen after elections but cannot be afterthoughts: evidence-based elections depend on them.

The other challenge is to frame requirements and test assertions that help to move auditability from an abstract possibility to a standard of excellence. One lesson of the Help America Vote Act era has been that a voting system may be formally “accessible” without being very usable by the voters who need it most. Similarly, a voting system may be “verifiable in name only” if its audit trail is difficult for voters to verify and/or for authorities to audit.

Voting systems should be rigorously tested to see if voters consistently and effectively verify their paper ballots or other auditable records in a variety of election conditions. (See the discussion of “ballots” below.) The systems also should be assessed for ease of auditability. The most auditable paper-based systems not only provide paper records that are easy for audit officials (as well as voters) to handle and to verify, but allow each paper record to be matched with the corresponding digital cast vote record(s) without compromising ballot anonymity.

Ballots and cast vote records: definitions and implications for auditability

In common parlance, ballots are paper records of voters’ votes, and cast vote records are digital representations of the votes on the ballots. To accommodate alternative models, the glossary that accompanies the VVSG defines “ballot” as a “presentation of the contest options for a particular voter,” and “cast vote record” as an “archival tabulatable record of all votes produced by a single voter from a given ballot.” In this framework, a ballot could be physical or digital, as could a cast vote record.

These expansive definitions seem to account for several confusing points in the principles and guidelines, such as 6.2’s reference to casting a cast vote record. They also complicate discussions of auditability. In a system based on paper ballots, the paper ballots can be verified and cast by voters and then audited. In systems that do not use paper ballots – even if they produce an auditable paper record – verifying and casting the ballot does not assure that the voter has verified the auditable record. If we could make just one change to the principles and guidelines, it would be to clarify in principle 7 and the associated guidelines that voters must be able to readily verify the records that will be retained and used to check whether the election outcome is correct (guideline 9.2).

Moreover, we believe that for the foreseeable future, only voter-verifiable paper records should be used for this purpose. Given the inherent vulnerabilities of today’s internet, no voting system that relies on digital records alone can provide truly secure and verifiable elections.

Specific comments

Principles 1 and 2: High Quality Design and Implementation

These principles are well framed, and we generally support the associated guidelines, particularly guideline 2.2 on user-centered design methods. Because most Americans vote no

more than once or twice per year, user-centered design is essential to provide systems that voters can use accurately and verifiably.

We believe that the guidelines should explicitly reference security as a crucial aspect of high-quality design. This can be accomplished by adding a new guideline 1.4, “Voting system design incorporates security best practices,” and by adding “best practices, including security best practices, in software development” in guideline 2.1.

Principle 3: Transparent

Guideline 3.1 refers to “security measures,” which ordinarily would refer to procedures rather than elements of voting system design. We suggest changing “security measures” to “security features.”

Principle 5: Equivalent and Consistent Voter Access

We support this principle. We recommend making explicit that guideline 5.1 extends to verification, for instance as follows: “Voters have a consistent experience throughout the voting process, including verification of the auditable records of their votes, in all modes of voting.” All voters deserve voting systems that facilitate verification.

Principle 6: Voter Privacy

We support this principle. We recommend revising guideline 6.2 to clarify, again, that the need for independent verification extends to whatever records will be used to audit tabulation accuracy. The phrase “ballot or other associated cast vote record” is too vague given the ambiguous definitions of both those terms. One possibility: “Voters can mark, verify and cast their ballot and other auditable records of their votes without assistance from others.

Principle 7: Marked, Verified, and Cast as Intended

“Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.” We doubt that vote selections (contest selections?) can be cast. We believe the intended meaning is something like “Ballots, including contest options and contest selections, are presented in a perceivable, operable, and understandable way; ballots can be marked, verified, and cast by all voters.”

We recommend adding a guideline to the effect that “The voting system allows voters to consistently and accurately verify their ballots and the auditable records of their votes.” Such a guideline lends itself to requirements and test assertions that support high levels of voter verification. Here is another place where voting system security will largely depend on election procedures, such as polling place layout and the instructions given to voters.

Guideline 7.2 enigmatically specifies that “voters have direct control of all ballot changes.” The intended meaning may be “voters have direct control of all ~~ballot changes~~ changes in their contest selections.”

Principle 8: Robust, Safe, Usable, and Accessible

In guideline 8.3, “measuring... for effectiveness, efficiency, and satisfaction” seems vaguely defined. We recommend language that evokes a rigorous performance standard, such as “~~for effectiveness, efficiency, and satisfaction~~ accuracy, efficiency, and satisfaction in marking, verifying, and casting their ballots.”

Principle 9: Auditable

We recommend revising guideline 9.2 to underscore that vote records used to verify outcomes should also be voter-verified. Moreover, for the foreseeable future, we would require these records to be physical. Also, a “correct” election outcome is undefined. We suggest: “The voting system produces readily available physical records that voters could verify. These records provide the ability to check whether the election outcome corresponds with voters’ contest selections and, to the extent possible, identify the root cause of any irregularities.”

In guideline 9.4, audit efficiency is desirable, but audit validity is paramount. We recommend expanding the guideline: “The voting system supports efficient, valid audits carried out with best practices.”

Principle 10: Ballot Secrecy

We agree with the comments of the Electronic Privacy Information Center (EPIC) in support of this principle. The term “ballot secrecy” is not included in the glossary, and its exact meaning is not self-evident: voted ballots themselves are not secret, and typically become public records once the election is complete. Verified Voting fully endorses the principle of ballot secrecy or ballot anonymity, as expressed in guideline 10.2: roughly, it should be impossible to tell how a particular person voted. We recommend defining this term in the glossary.

Principle 13: Data Protection

This principle, and guideline 13.4, appear to use “sensitive data” to refer both to data that should not be revealed due to privacy or confidentiality concerns, and data that is critical to the integrity of the election but not “sensitive” from a privacy standpoint. We suggest deleting “sensitive” from the principle (no data should be subject to “unauthorized access, modification, or deletion”), and drawing the distinction in guideline 13.4: for instance, “The voting system protects the integrity and authenticity of all data, and the confidentiality of sensitive data, transmitted over all networks.”

Principle 14: System Integrity

Guideline 14.2 appears to be missing a word: "...by reducing unnecessary code, data paths, and physical ports, and by using other technical controls." We further recommend replacing "reducing" with "avoiding" or "eschewing."

We concur with the recommendation of EPIC, the State Audit Working Group (SAWG), and others to add a new guideline (or add to 14.2): "The voting system does not use wireless technology or connect to any public telecommunications infrastructure." These risks are best eliminated.

In guideline 14.3, we concur with the SAWG proposal to insert: "The voting system maintains and verifies, and facilitates independent human verification of, the integrity of software, firmware, and other critical components." Systems should not be relied upon to verify themselves.

Principle 15: Detection and Monitoring

Guidelines 15.3 and 15.4 seem to go beyond the scope of the associated principle. It may be appropriate to add "prevention" to the principle or to narrow these guidelines, perhaps broadening guidelines associated with other principles accordingly.

About Verified Voting

Verified Voting (www.verifiedvoting.org), founded by computer scientists in 2004, is a leading national not-for-profit, non-partisan organization focused exclusively on the critical role technology plays in election administration. Through education and advocacy, our mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology and election administration experts who comprehend the risks associated with the emerging digital landscape, particularly the online and electronic elements in voting. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.



Verified Voting.org

Public Comments on VVSG 2.0 Principles and Guidelines

Submitted May 29, 2019

Verified Voting is pleased to see the VVSG 2.0 principles and guidelines finally moving forward. We are enthusiastic about the VVSG 2.0 structure and, with some reservations, about the content of the principles and guidelines. Full implementation of the VVSG 2.0 will, in time, help bring about voting systems that set new standards for universal usability, security, and verifiability. All these properties – backed by sound procedures – are essential to enable officials to run resilient elections, and to reassure voters that their votes have been cast as intended and counted as cast.

We urge the EAC to allow the technical requirements and test assertions to be approved and revised without a vote of the commissioners. We agree with the TGDC, the NASED executive council, and others that for several reasons, these documents are best managed by technical staff, adhering to a well-defined process with broad consultation and opportunity for public comment.

Verification and the VVSG

Verified Voting especially welcomes Principle 9, which stipulates that a voting system “is auditable and enables evidence-based elections,” and the associated guidelines. No matter how otherwise usable and reliable a voting system may be, it is unacceptably dangerous if it cannot provide trustworthy, software-independent evidence that people’s votes have been accurately recorded and counted.

A voting system alone can “enable” evidence-based elections but cannot provide them. As Philip Stark and David Wagner wrote in their seminal paper, the basic equation is that “evidence = auditability + auditing.” A voting system with a voter-verifiable audit trail, such as a voter-marked paper ballot, provides auditability. Compliance audits to ensure that the audit trail is substantially complete and accurate, and risk-limiting tabulation audits of the audit trail, provide actual evidence that outcomes are correct.

These considerations point to two ongoing challenges for the EAC and everyone else who works with the VVSG. One challenge is to communicate

that, in practice, voting system security largely depends on election procedures and especially on post-election audit procedures. Compliance and risk-limiting tabulation audits happen after elections but cannot be afterthoughts: evidence-based elections depend on them.

The other challenge is to frame requirements and test assertions that help to move auditability from an abstract possibility to a standard of excellence. One lesson of the Help America Vote Act era has been that a voting system may be formally “accessible” without being very usable by the voters who need it most. Similarly, a voting system may be “verifiable in name only” if its audit trail is difficult for voters to verify and/or for authorities to audit.

Voting systems should be rigorously tested to see if voters consistently and effectively verify their paper ballots or other auditable records in a variety of election conditions. (See the discussion of “ballots” below.) The systems also should be assessed for ease of auditability. The most auditable paper-based systems not only provide paper records that are easy for audit officials (as well as voters) to handle and to verify, but allow each paper record to be matched with the corresponding digital cast vote record(s) without compromising ballot anonymity.

Ballots and cast vote records: definitions and implications for auditability

In common parlance, ballots are paper records of voters’ votes, and cast vote records are digital representations of the votes on the ballots. To accommodate alternative models, the glossary that accompanies the VVSG defines “ballot” as a “presentation of the contest options for a particular voter,” and “cast vote record” as an “archival tabulatable record of all votes produced by a single voter from a given ballot.” In this framework, a ballot could be physical or digital, as could a cast vote record.

These expansive definitions seem to account for several confusing points in the principles and guidelines, such as 6.2’s reference to casting a cast vote record. They also complicate discussions of auditability. In a system based on paper ballots, the paper ballots can be verified and cast by voters and then audited. In systems that do not use paper ballots – even if they produce an auditable paper record – verifying and casting the ballot does not assure that the voter has verified the auditable record. If we could make just one change to the principles and guidelines, it would be to clarify in principle 7 and the associated guidelines that voters must be able to readily verify the records that will be retained and used to check whether the election outcome is correct (guideline 9.2).

Moreover, we believe that for the foreseeable future, only voter-verifiable paper records should be used for this purpose. Given the inherent vulnerabilities of today’s internet, no voting system that relies on digital records alone can provide truly secure and verifiable elections.

Specific comments

Principles 1 and 2: High Quality Design and Implementation

These principles are well framed, and we generally support the associated guidelines, particularly guideline 2.2 on user-centered design methods. Because most Americans vote no

more than once or twice per year, user-centered design is essential to provide systems that voters can use accurately and verifiably.

We believe that the guidelines should explicitly reference security as a crucial aspect of high-quality design. This can be accomplished by adding a new guideline 1.4, “Voting system design incorporates security best practices,” and by adding “best practices, including security best practices, in software development” in guideline 2.1.

Principle 3: Transparent

Guideline 3.1 refers to “security measures,” which ordinarily would refer to procedures rather than elements of voting system design. We suggest changing “security measures” to “security features.”

Principle 5: Equivalent and Consistent Voter Access

We support this principle. We recommend making explicit that guideline 5.1 extends to verification, for instance as follows: “Voters have a consistent experience throughout the voting process, including verification of the auditable records of their votes, in all modes of voting.” All voters deserve voting systems that facilitate verification.

Principle 6: Voter Privacy

We support this principle. We recommend revising guideline 6.2 to clarify, again, that the need for independent verification extends to whatever records will be used to audit tabulation accuracy. The phrase “ballot or other associated cast vote record” is too vague given the ambiguous definitions of both those terms. One possibility: “Voters can mark, verify and cast their ballot and other auditable records of their votes without assistance from others.”

Principle 7: Marked, Verified, and Cast as Intended

“Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.” We doubt that vote selections (contest selections?) can be cast. We believe the intended meaning is something like “Ballots, including contest options and contest selections, are presented in a perceivable, operable, and understandable way; ballots can be marked, verified, and cast by all voters.”

We recommend adding a guideline to the effect that “The voting system allows voters to consistently and accurately verify their ballots and the auditable records of their votes.” Such a guideline lends itself to requirements and test assertions that support high levels of voter verification. Here is another place where voting system security will largely depend on election procedures, such as polling place layout and the instructions given to voters.

Guideline 7.2 enigmatically specifies that “voters have direct control of all ballot changes.” The intended meaning may be “voters have direct control of all ~~ballot changes~~ in their contest selections.”

Principle 8: Robust, Safe, Usable, and Accessible

In guideline 8.3, “measuring... for effectiveness, efficiency, and satisfaction” seems vaguely defined. We recommend language that evokes a rigorous performance standard, such as “~~for effectiveness, efficiency, and satisfaction~~ accuracy, efficiency, and satisfaction in marking, verifying, and casting their ballots.”

Principle 9: Auditable

We recommend revising guideline 9.2 to underscore that vote records used to verify outcomes should also be voter-verified. Moreover, for the foreseeable future, we would require these records to be physical. Also, a “correct” election outcome is undefined. We suggest: “The voting system produces readily available physical records that voters could verify. These records provide the ability to check whether the election outcome corresponds with voters’ contest selections and, to the extent possible, identify the root cause of any irregularities.”

In guideline 9.4, audit efficiency is desirable, but audit validity is paramount. We recommend expanding the guideline: “The voting system supports efficient, valid audits carried out with best practices.”

Principle 10: Ballot Secrecy

We agree with the comments of the Electronic Privacy Information Center (EPIC) in support of this principle. The term “ballot secrecy” is not included in the glossary, and its exact meaning is not self-evident: voted ballots themselves are not secret, and typically become public records once the election is complete. Verified Voting fully endorses the principle of ballot secrecy or ballot anonymity, as expressed in guideline 10.2: roughly, it should be impossible to tell how a particular person voted. We recommend defining this term in the glossary.

Principle 13: Data Protection

This principle, and guideline 13.4, appear to use “sensitive data” to refer both to data that should not be revealed due to privacy or confidentiality concerns, and data that is critical to the integrity of the election but not “sensitive” from a privacy standpoint. We suggest deleting “sensitive” from the principle (no data should be subject to “unauthorized access, modification, or deletion”), and drawing the distinction in guideline 13.4: for instance, “The voting system protects the integrity and authenticity of all data, and the confidentiality of sensitive data, transmitted over all networks.”

Principle 14: System Integrity

Guideline 14.2 appears to be missing a word: "...by reducing unnecessary code, data paths, and physical ports, and by using other technical controls." We further recommend replacing "reducing" with "avoiding" or "eschewing."

We concur with the recommendation of EPIC, the State Audit Working Group (SAWG), and others to add a new guideline (or add to 14.2): "The voting system does not use wireless technology or connect to any public telecommunications infrastructure." These risks are best eliminated.

In guideline 14.3, we concur with the SAWG proposal to insert: "The voting system maintains and verifies, and facilitates independent human verification of, the integrity of software, firmware, and other critical components." Systems should not be relied upon to verify themselves.

Principle 15: Detection and Monitoring

Guidelines 15.3 and 15.4 seem to go beyond the scope of the associated principle. It may be appropriate to add "prevention" to the principle or to narrow these guidelines, perhaps broadening guidelines associated with other principles accordingly.

About Verified Voting

Verified Voting (www.verifiedvoting.org), founded by computer scientists in 2004, is a leading national not-for-profit, non-partisan organization focused exclusively on the critical role technology plays in election administration. Through education and advocacy, our mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology and election administration experts who comprehend the risks associated with the emerging digital landscape, particularly the online and electronic elements in voting. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.



June 6, 2019

Fish & Richardson P.C.
12390 El Camino Real
San Diego, CA 92130
858 678 5070 main
858 678 5099 fax

VIA FEDERAL EXPRESS

Clifford Tatum, General Counsel
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Michael A. Amon
Principal
amon@fr.com
858 678 4708 direct

Dear Mr. Tatum:

I am a partner with Fish & Richardson, P.C., a nationwide leading law firm focusing on intellectual property issues. I represent clients across a wide array of industries, including clients in the voting machine industry. We have extensive experience in patent licensing and patent litigation, and have worked on numerous matters involving standards-essential patents (SEPs).

I write today on behalf of our clients in the voting machine industry to express some concerns regarding the Election Assistance Commission's development of new technical standards for voting machines (VVSG 2.0). While our clients agree with the EAC's development of a set of standardized technologies for voting machine systems that will allow for secure and accessible elections across the country, our clients are concerned that the incorporation of patented technology into the standards will limit competition and create a de-facto monopoly in the voting machine industry. We and our clients want to try to ensure that the EAC implements appropriate safeguards against monopolization of standardized voting machine technologies, including by considering whether technologies are patented prior to adoption into the standard and by asking stakeholders whose patented technology may be incorporated into the standards to make a commitment to license that technology on fair, reasonable, and non-discriminatory terms.

As you may be aware, a patent is a federally-granted intellectual property right that entitles its owners to exclude others from practicing technology covered by a patent's claims. *See, e.g., Dawson Chem. Co. v. Rohm & Haas Co.*, 448 U.S. 176, 215 (1980) (noting "the long-settled view that the essence of a patent grant is the right to exclude others from profiting by the patented invention"); *see also* 35 U.S.C. § 154(a)(1) (giving a patentee the "right to exclude others from making, using, offering for sale, or selling the [patented] invention"). In enforcing this right to exclude, district courts "may grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent, on such terms as the court deems reasonable." 35 U.S.C. § 283. "[N]ot surprising[ly], given the difficulty of protecting a right to *exclude* through monetary remedies that allow an infringer to use an invention against the patentee's wishes," historically courts have "granted injunctive relief upon a finding of infringement in the vast majority of patent cases." *eBay Inc. v. MercExchange*,

L.L.C., 547 U.S. 388, 395 (2006) (Roberts, C.J., concurring) (emphasis in original). Alternatively, the patent owner may demand such a high royalty to access the patented technology that the royalty effectively acts to quash competition in the market. If the EAC adopts technology covered by a patent, that patent owner could potentially enforce the right to exclude granted by the patent through an injunction, or demand such a high royalty so as to foreclose competitors from creating voting systems that comport with the standards. And, because complying with EAC standards is required for certification of voting machine systems—which allows a company to sell the machines—a single patent owner could potentially exclude all competitors from the entire market, creating a de facto monopoly.

Our clients' concerns regarding voting machine patents is far from speculative. A brief search on Google Patents reveals over 2,000 patents covering voting machine technology.¹ Certain companies have recently turned to the courts to enforce their patent rights covering voting machine technology, bringing suit against competitors and even municipalities seeking damages and potentially the right to exclude others through the operation of an injunction. See, e.g., *Election Systems & Software, LLC v. Smartmatic USA Corporation*, Case No. 1-18-cv-01259 (D. Del. 2018); *Election Systems & Software, LLC v. Unisyn Voting Solutions, Inc.*; Case No. 3-18-cv-00910 (S.D. Cal. 2018); *Election Systems & Software, LLC v. Dominion Voting Systems, Inc.*, Case No. 1-17-cv-01172 (D. Del. 2017); *Voter Verified, Inc. v. Election Systems & Software, LLC f/k/a Election Systems & Software, Inc.*; Case No. 1-16-cv-00267 (N.D. Fl. 2016).

Competition in the voting machine industry is essential to maintaining vibrant and secure elections in the United States. A concentrated market structure in the voting machine industry can threaten the integrity of our elections because, among other reasons, a company that has a monopoly over voting machines has limited incentives to innovate, including in the security of our vote.² The reasons for this are plain – if a company no longer has to compete to earn customers, the drive to innovate and offer new and improved functionality and security evaporate. If a company is allowed to use its patents to exclude others from the voting machine marketplace, the resulting monopoly will threaten our democracy. That said, our clients understand that companies that invest in and develop new technologies should be rewarded for those efforts. Thus, in developing mechanisms relating to patents, the EAC should attempt to strike a balance between rewarding innovators and protecting competition.

¹ See <https://patents.google.com/?q=%22voting+machine%22&oq=%22voting+machine%22>.

² See Gutierrez, German & Thomas Philippon, "Declining Competition and Investment in the U.S.," available at https://www8.gsb.columbia.edu/faculty-research/sites/faculty-research/files/finance/Macro%20Lunch/IK_Comp_v1.pdf (finding that "industries with less competition and more concentration (traditional or due to common ownership) invest less" in new technologies").

The voting machine industry is not the first industry to face this issue. Industries standards are commonplace in other technology areas, including cell phone technology, Wi-Fi, Bluetooth, and others where multiple companies have to create interoperable parts. These industries have worked together to protect competition while rewarding patent owners. Generally, all of these industries have arrived at very similar answers, with two important components: (1) requiring stakeholders to disclose patents that potentially read on technology that may become part of a standard (SEPs); and (2) requiring patent owners to pledge to license SEPs to all stakeholders on fair, reasonable, and non-discriminatory terms (“FRAND”).³ Requiring disclosure allows the body developing the standards to know whether technology incorporated into the standard is covered by a patent, thus allowing the standards body to make an informed choice regarding what technologies to incorporate into the required standard. Requiring the FRAND commitment ensures that no one company can use patents to exclude others from using the standard, or to allow that company to discriminate against certain competitors and exert an undue influence over the marketplace.

Our clients urge the EAC to adopt similar requirements in establishing the standards for voting machine systems. All stakeholders, and especially companies who make contributions or urge the adoption of a particular standard, should be required to disclose whether they own patents that cover standardized technology. Similarly, stakeholders should be required to make FRAND commitments for any patents that cover standardized technology adopted for voting machine systems. Our clients feel that these are necessary steps to continue a vibrant marketplace, to ensure continued competition in the voting machine industry, and to protect the integrity of our elections.

Best regards,



Michael A. Amon

cc: Dr. Walter G. Copan, Under Secretary of Commerce for Standards and Technology and NIST Director;
Brian Newby, Executive Director of the EAC;
Jerome Lovato, Testing & Certification Director of the EAC;
Mona Harrington, Chief Information Officer of the EAC.

³ See, e.g., the “Intellectual Property Rights” policy of the European Telecommunications Standards Institute, which is the industry group that sets standards for the cell phone industry, available at <https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf>.



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

PUBLIC COMMENT PERIOD FOR VOTING SYSTEM GUIDELINES

1 message

Karen Corley <[REDACTED]>

To: votingsystemguidelines@eac.gov

Fri, Mar 1, 2019 at 6:27 PM

I have a comment. I would add to the voting system guidelines that BARCODE-type ballots be **prohibited in every state**. They are too prone to hacking and security issues. Simple paper ballots are best! That's what my community uses and we have no problems! With all the foreign interference and hacking, let's go with the tried and true method of voting!

Karen and Christopher Corley
[REDACTED]

Webster Groves, MO 63119



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

Comment on Voluntary Voting System Guidelines 2.0

1 message

Patricia Castellano <[REDACTED]>

Sat, Mar 2, 2019 at 9:54 AM

To: votingsystemguidelines@eac.gov

1. Paper ballots, please. Not only ballot-marking devices for disabled, but everyone marks their own ballot.
2. No bar code voting (what are safeguards to check the accuracy of the voting? Easy to change bar codes)
3. No DRE's (principles are well and good, but equipment counts)
4. Handmarked paper ballots (redundant but cannot stress enough)

Pat Castellano CHES



Voluntary Voting System Guidelines 2.0

Principles and Guidelines

Principle 1: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

- 1.1** - The voting system is designed using commonly-accepted election process specifications.
- 1.2** - The voting system is designed to function correctly under real-world operating conditions.
- 1.3** - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

Principle 2: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

- 2.1** - The voting system and its software are implemented using trustworthy materials and best practices in software development.
- 2.2** - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers.
- 2.3** - Voting system logic is clear, meaningful, and well-structured.
- 2.4** - Voting system structure is modular, scalable, and robust.
- 2.5** - The voting system supports system processes and data with integrity.
- 2.6** - The voting system handles errors robustly and gracefully recovers from failure.
- 2.7** - The voting system performs reliably in anticipated physical environments.

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

- 3.1** - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.
- 3.2** - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.
- 3.3** - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

- 4.1** - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.
- 4.2** - Standard, publicly-available formats for other types of data are used, where available.
- 4.3** - Widely-used hardware interfaces and communications protocols are used.
- 4.4** - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities, without discrimination.

- 5.1** - Voters have a consistent experience throughout the voting process in all modes of voting.
- 5.2** - Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

- 6.1** - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.
- 6.2** - Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware and accessories protect users from harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 The voting system is evaluated for usability by election workers.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Principle 11: ACCESS CONTROL

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION

The voting system protects sensitive data from unauthorized access, modification, or deletion.

- 13.1** –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.
- 13.2** - The source and integrity of electronic tabulation reports are verifiable.
- 13.3** - All cryptographic algorithms are public, well-vetted, and standardized.
- 13.4** - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

- 14.1** - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.
- 14.2** - The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls.
- 14.3** - The voting system maintains and verifies the integrity of software, firmware, and other critical components.
- 14.4** - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING

The voting system provides mechanisms to detect anomalous or malicious behavior.

- 15.1** - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.
- 15.2** - The voting system generates, stores, and reports all error messages as they occur.
- 15.3** - The voting system employs mechanisms to protect against malware.
- 15.4** - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

VVSG 2.0

1 message

'Bettina Maravolo' via Voting System Guidelines <votingsystemguidelines@eac.gov>

Fri, Apr 19, 2019 at 12:03 PM

Reply-To: Bettina Maravolo <[REDACTED]>

To: "votingsystemguidelines@eac.gov" <votingsystemguidelines@eac.gov>

To Whom It May Concern,

I support the VVSG. Notably, the guidelines require that voters understand all documentation on the voting system and all information presented on the ballot are commendable.

I sincerely appreciate the EAC updating the voting system standards.

Regards,

Bettina Maravolo



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

I Support the VVSG 2.0

1 message

Sam Jared Bonar <[REDACTED]>

To: votingguidelines@eac.gov

Fri, Apr 19, 2019 at 4:33 PM

Hello!

I am a voting rights and election security advocate who has 5 years of experience as a government analyst and 4 years as an advocate and activist around my community in DC.

I am writing to express support for these strengthened guidelines and standards for our elections as soon as possible. We need as much teeth to make sure states guarantee transparency, high quality design and usability, audit-ability, and interoperability.

I would also like to urge you to add and clarify requirements for voting systems to be able to handle alternative voting systems (such as Ranked Choice Voting and Star Voting) that would improve voter choice.

Thank you!

Sam Bonar



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

Comments for VVSG 2.0 Comment Period

1 message

Lauren Galanter [REDACTED] >

Fri, Apr 19, 2019 at 6:14 PM

To: votingsystemguidelines@eac.gov

Hi,

I would like to submit my strong support for the current VVSG 2.0 draft. Most important to me are Principles 1 and 2 for high-quality design and implementation that employ best practices in user-centered design.

Sincerely,
Lauren Galanter
User Experience Designer and Researcher
Philadelphia, PA



U.S.ELECTION
ASSISTANCE
COMMISSION

Ryan Macias <rmacias@eac.gov>

Comments for VVSG 2.0 Comment Period

1 message

Elizabeth Kim <[REDACTED]>

Mon, Apr 22, 2019 at 10:31 AM

To: votingsystemguidelines@eac.gov

Hello, this is very exciting. Thank you for giving others a chance to participate in this process. These guidelines set a very admirable standard for designers everywhere!

1) What does "the voting system" include? Is it just the stuff that happens when the user is at a site ready to cast a ballot? It could be helpful to include this at the top of the guidelines.

I ask this because I am wondering if...

2) principle 5: there should be a note about how everyone should have the same degree of access, ability and convenience as anyone else regardless of income/place of work, access to transportation, etc. In reaching voting sites or accessing information about the vote? (Not disability related. More about a voter's non-physical/mental circumstances.)

3) principle 4 /13- add something about privacy how data should or should not be used?

I read through this pretty quickly but please forgive me if I've mentioned something which has already been considered.

Elizabeth Kim, product designer. Design practitioner since 2012. Graduate of Parsons school of Design.

Comments on draft VVSG 2.0

P.B. Stark

Prepared for the EAC Public Hearing on VVSG 2.0

Salt Lake City, Utah

23 April 2019 (Last edited 29 April 2019)

This document is a slightly extended version of comments presented in oral testimony at the 23 April 2019 hearing on draft VVSG 2.0.

- I am limiting my comments to the principles, not the guidelines.
- Overall, the principles in VVSG 2.0 are terrific and I strongly endorse them.
- I strongly support separating principles from detailed technical requirements.
- However, the devil is often in the details—in this case, the detailed requirements that will flow from the principles and guidelines.
- As far as I know, there is as yet no process to ensure that the detailed requirements embody the VVSG and do not contradict it.
- My primary concerns with the VVSG Principles themselves regard language that is ambiguous and wording that suggests that future voting systems will not use hand-marked paper ballots—the most secure, trustworthy, and resilient mode of voting currently available.
- I also recommend that the VVSG include a precise glossary to define important terms including “ballot,” “cast,” “cast vote record,” “audit,” and “physical port.” While the definitions in the VVSG might conflict with the use of those terms in state laws, it is necessary for the VVSG to be completely clear; the use of that language of course is not binding on states. Language concerning the “secrecy” of ballots and votes versus the “anonymity” of ballots could also be improved: voters should vote privately and there should be no way to link votes to individual voters, but votes should be anonymous rather than secret.

I now comment on specific principles.

Principle 4: INTEROPERABLE The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

- This is critical for establishing a truly competitive market for voting systems, to facilitate innovation, and to facilitate meaningful audits of election results.
- Software to support efficient tabulation audits, such as risk-limiting audits, will need to parse exported results and exported cast vote records, for instance.
- Interoperability is also critical to enable more modular certification decisions, so that eventually, individual components rather than monolithic systems can be certified. That can facilitate the deployment of technology improvements and security improvements and make maintenance and upgrades cheaper and easier.

5.1 Voters have a consistent experience throughout the voting process in all modes of voting.

- This could be read to imply that all voters should use the same technology to mark and cast ballots, which could reduce usability for some groups of voters.
- Each voter should be provided a means of marking, verifying, and casting a ballot that is as usable by that voter as possible.

5.2 Voters receive equivalent information and options in all modes of voting.

- This implies that the system should provide voters with disabilities a means to verify independently that what is printed on the paper record matches their selections. It would be good to spell that out explicitly.

6.2 Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

- Voters do not “cast” or “mark” cast vote records; voters cannot see, touch, or verify cast vote records.
- Voting equipment creates a cast vote record from voter input. CVRs are the system’s internal electronic representation of the voter’s selections.

- There is no guarantee that the cast vote record matches the voter's input, what the voter saw on the screen, or what was printed on the ballot. Indeed, one way of conducting a risk-limiting audit involves checking whether CVRs accurately reflect what is printed on the corresponding ballot.
- This is another example of language that needs to be tightened.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

- Again, this should include a provision to ensure that voters with disabilities are provided a means to verify independently that what is printed on the paper record accurately reflects their selections.
- On-screen (or audio) verification before the paper record has been printed is not sufficient, because the system could print something different on the paper record, as a result of bugs, misconfiguration, or hacking.
- Again, the language in this principle lacks precision: "vote selections" are not cast. Ballots are cast.

7.1 The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

- This implies that all voters will vote using an electronic interface, which would be detrimental to election integrity and security.
- I suggest revising the wording to include requirements for usability of hand-marked paper ballots.

7.2 Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

- This implies that ballots, rather than ballot presentation formats, are controlled by the voter.
- The voter should have control over some aspects of the format of the presentation of information for the purpose of making selections.
- This is another example where the draft language is not consistent. The "ballot" is a piece of paper that records the voters' selections, not a screen that presents the voter options.

8.3 The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

- “Effectiveness” and “efficiency” need workable definitions.
- How does one trade off between speed and accuracy?
- Measuring things is great—if they are well defined—but what action does this lead to? How do these measurements affect whether a voting system can be certified?
- The system should be tested for accuracy in capturing voter intent and for ease of use, both for recording votes and for verifying selections on the paper ballot, for representative voters, including voters with and without disabilities.
- Satisfaction is desirable, but accuracy and ease of use are essential.
- Analogously, good bedside manner increases patient satisfaction with doctors, but first and foremost, we need doctors to be competent.

8.4 The voting system is evaluated for usability by election workers.

- This should include usability for auditing election outcomes, not just for conducting the election.
- Is “evaluation” enough? Presumably there is a minimum level of usability that should be required for certification.

9.4 The voting system supports efficient audits.

- This is rather vague. What constitutes an audit? What is to be audited? What does it mean for an audit to be “efficient”—what is it to be compared to?
- The definition of “audit” varies widely across jurisdictions. Some jurisdictions consider examining a transaction log to be an audit. While that is valuable, it is not sufficient to establish that contest outcomes are correct. The same is true for logic and accuracy testing (LAT), and for “audits” based on inspecting digital images of ballots, rather than the original voter-verified paper records.
- The system should support efficient audits of the integrity of the paper trail and the accuracy of the tabulation and the reported results, at a minimum.

- We need systems to support audits that can detect whether the evidence trail has been compromised and that can correct wrong reported outcomes, for instance, so-called “compliance” audits of the integrity of the paper trail. combined with rigorous risk-limiting audits of the tabulation. Here is some terminology, for reference:
 - A *compliance audit* establishes whether the paper trail is trustworthy.
 - A *risk-limiting audit* (RLA) ensures that if tabulation errors caused the wrong candidate or position to appear to win, there is a large chance of correcting the outcome before it is certified. RLAs involves manually inspecting a random sample of paper records. If a compliance audit has demonstrated that the paper trail is trustworthy, a RLA has a known probability of correcting the outcome if the outcome is wrong, no matter why it is wrong.
- RLAs are most efficient when the voting system can export a cast vote record (CV) for each physical ballot, in a way that the ballot that corresponds to a given CVR is uniquely identified, and vice versa. That makes it possible to check the voting system’s interpretation of individual ballots. It would be facilitate efficient audits if the VVSG required voting systems to create and export a CVR for every physical ballot, in such a way that the corresponding physical ballot is uniquely identified and can be retrieved for manual inspection.

10.1 Ballot secrecy is maintained throughout the voting process.

- Ballots are public records of a sort.
- Votes should be anonymous, not secret.
- The contents of at least some ballots need to be seen by election officials and auditors, but there should be no way to know who cast which ballot.
- This is another example where the language should be tightened.

Principle 13 and Principle 14.2

- Together, these *should* imply that voting systems shall not have wireless connections such as bluetooth, WiFi, or cellular communication ports.
- Is a wireless interface considered a “physical port”? There is no definition of “physical port.”
- Will the requirements reflect that?

- I recommend that the VVSG prohibit radios of any kind in equipment used to mark ballots, record votes, or tabulate votes. Such wireless communication hardware should not be present in those devices: disabling it in software is not an adequate precaution.

15.4 A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

- No system for capturing or tabulating votes should ever be connected to the Internet, nor to a private network that is connected to the Internet, nor to any other public communications infrastructure.
- No system for marking ballots or capturing or tabulating votes should have “remote desktop software” installed.

May 7th, 2019

US Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Springs, Maryland 20910

To Whom it May Concern:

Do you have a teenager at home? On a scale from 1-10, how responsible would you say they are? How responsible do you believe teenagers are in general? How many times do you hear the word, “teenager” and think these three words in your head, “good citizen”, “responsible and mature”, and “changing their community”? Some may believe their teenager is all these and more, and that’s great. But according to pewinternet.com, “61% of parents feel the need to monitor their teenager’s activity online, and during the day, because they do not feel that their child is responsible or mature enough to handle larger responsibility. One thing our country can do to change that, is to allow teenagers, ages 15 and older to vote. Currently, our voting laws state that you must be 18 on, or before election dates to register to vote, but allowing 15-year-old American citizens to vote would lead to many wonderful benefits. Teenagers will learn to be better citizens, become more responsible and politically mature, and be influenced to participate in their community. Changing this law would greatly benefit the young people of America.

First of all, teenagers will learn to be better citizens. Lowering the voting age would help teenagers develop habits of a good citizen and continue to influence others of their age to do the same. Decreasing the voting age would lead to a long-term increase in voter turnout, bringing more citizens in touch with their government and pushing the government to better serve its people. According to a recent study, “A person who votes in the first election they are eligible for, is more likely to continue to vote constantly, while someone who doesn’t will take several years to pick up the habit.” It is clear, that age 15 is a better time to establish a new habit than at age 18, and data from places that have lowered the voting age show that 15-year-old citizens do indeed vote at higher rates than first time voters. Not only would lowering the voting age assist teenagers in developing great political habits, but changing this law would also help our government receive more diverse opinions from a younger age group, which would be beneficial for our society.

Even more so, decreasing the voting age to 15 would greatly benefit all teenagers, parents, teachers, and anybody in the environment of teenagers, because teenagers would show more responsibility and become politically mature. According to Psychologytoday.com “studies with American teens have found 15-17-year-olds having similar, (and in some cases greater) political efficiency, knowledge, interest, tolerance, and skills than 18-year-olds.” Psychologytoday.com also said that, “It is true that classrooms allowing teenagers to cast “mock votes” have teens with higher civic knowledge and more intent to vote in the future. These findings would suggest that

lowering the voting age to 15 would increase “political maturity in youths today and encourage them to make responsible decisions.

In addition to creating better citizens and encouraging responsibility in teenagers, decreasing the voting age would result in teenagers being more influenced to participate in their community. All people are affected by the decision’s politicians make and allowing teens to vote would allow them to have a say in their community. Daisy Berru, age 17, from layouth.com says, “People who don’t want teenagers to vote may believe that teens would not take the privilege seriously, and they wouldn’t really care about what they were taking part in. But teenagers who would not care would most likely not be participating anyway.” By not allowing teenagers to vote because of this belief, you are preventing the teenagers who care about having a say on the decisions impacting their country from making their opinions heard. Seth Falcon, age 14, also from layouth.com agrees with Daisy Berru and says, “Many teens are well informed and mature. Allowing them to vote would allow teenagers to have a say in their community, and even the changes being made in the country they are growing up in.” This proves that teenagers really do want to have a say on the changes being made in their country, and lowering the voting age would allow them to do that.

Lowering the voting age to 15 would be a worthwhile decision and you would be astonished by the supportive results. By following through with this proposal, you would allow American teenagers to become better citizens, become more responsible and politically mature, all while influencing them to participate in their community. Lowering the voting age has wide support. According to youthrights.org, “Nearly half of the United States have seen legislative attempts to lower the voting age to 15 in the last 25 years!” Teenagers are given adult responsibilities, but they are not given adult rights. If you agree with that, don’t you also believe that children are the future, so they should be allowed to vote? I urge you to consider this proposal and think about all the benefits lowering the voting age would have on American society.

Sincerely,



Ella Brinkman



Comments on the VVSG 2.0 Principles and Guidelines

We enthusiastically support the new VVSG 2.0 principles and guidelines as a strong framework for the next version of federal voting system standards that will make the detailed requirements easier to understand and encourage innovations in voting system design. We hope that the new VVSG will be approved quickly, to allow voting system designers and elections offices across the country to take advantage of it.

We respectfully suggest two edits to the VVSG 2.0 guidelines to make them clearer and avoid ambiguity.

1.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

8.1 - The voting system's hardware and accessories protect users from harmful conditions.

Although the principle includes "robust" (from the Web Content Accessibility Guidelines), and the word "safe" (from VVSG 1.1) the term is not used in any of the guidelines in Principle 8.

We suggest editing Guideline 8.1 to add the words "robust and safe" to help identify the guideline and underlying requirements that address these topics.

8.1 - The voting system's hardware, software, and accessories are **robust and safe, protecting** users from harmful conditions.

2.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 - The voting system is evaluated for usability by election workers.

The text of Guideline 8.4 can be read to mean that the evaluation is conducted *by* election workers rather than the intended meaning of evaluating the experience the workers have using the system.

We suggest editing Guideline 8.4 and Guideline 8.3 (usability for voters). For example, we thought of the following alternatives to make the meaning clearer.

8.3 - The voting system is **evaluated** with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 - The voting system is evaluated for usability **for** election workers.

8.4 - The voting system is evaluated **with election workers** for usability.

8.4 - The voting system is evaluated **with** election workers for usability **of administrative interfaces**.

Thank you,



Dana Chisnell
Co-Director, Center for Civic Design

May 14, 2019



U.S.ELECTION
ASSISTANCE
COMMISSION

Jerome Lovato <jlovato@eac.gov>

Support for Voluntary Voting System Guidelines 2.0 Principles and Guidelines

1 message

Kelly Delahanty [REDACTED] >

Wed, May 15, 2019 at 11:29 AM

To: votingsystemguidelines@eac.gov

I support VVSG 2.0. As a user experience designer, I believe that making sure that strong user-centric principles are applied to voting - the most important aspect of our democracy - is incredibly important. The voting process should be accessible, secure, up-to-date, and user-friendly. I acted as a pollwatcher in the 2018 election as was shocked at how difficult it was for the trained election judges to use the voting system and the ways in which the voting process was not accessible to people with disabilities. I hope that these new guidelines will improve the situation.

-Kelly

--

Kelly Delahanty
(630) 244-6799
kellydelahanty@gmail.com
kellydelahanty.com



U.S.ELECTION
ASSISTANCE
COMMISSION

Jerome Lovato <jlovato@eac.gov>

Testimony on proposed VVSG 2.0 Principles and Guidelines.

2 messages

Guillermo Mena [REDACTED] >

To: "votingsystemguidelines@eac.gov" <votingsystemguidelines@eac.gov>

Fri, May 17, 2019 at 4:32 PM

Dear members of the US Election Assistance Commission,

I hereby request a slot to testify on behalf of NHCSL—The National Hispanic Caucus of State Legislators, at the hearing to be held on May 20, 2019 regarding the Voluntary Voting System Guidelines 2.0 Principles and Guidelines (VVSG 2.0). My testimony will be IN OPPOSITION to the proposed VVSG 2.0.

Contact Information:

Guillermo Mena

Director of Legislation, Policy and Advocacy

NHCSL - The National Hispanic Caucus of State Legislators

Email: gmena@nhcsl.org

Description of what will be said:

1. The proposed VVSG 2.0 contains language that can lead to unintended consequences and/or is too vague to be useful, such as “best practice,” “commonly-accepted election process specifications,” “wide range of representative voters,” “widest range of voters,” “widest range of representative voters,” “currently accepted federal standards,” “consistent experience... in all modes of voting” and the use of the word “ballot” to apparently refer to at least two things which could be different: what is displayed to the voter, and what is finally cast.
2. The proposed VVSG 2.0 does not meet the needs of paper ballot systems, treating them at best as an afterthought (for example requiring that “voters can adjust settings and preferences to meet their needs,” or “configurable authentication mechanisms,” “equivalent... options in all modes of voting,” or entire lines that seem to address only electronic systems without differentiating the front-end systems that voters interact with and the back-end reporting and aggregation systems that all systems include), even though HAVA underscores that paper ballot systems are protected under the Act.
3. The proposed VVSG 2.0 fails to define minimally acceptable requirements for many terms such as “settings,” “preferences,” “measured,” “effectiveness,” “efficiency,” “satisfaction,” “best practice,” and “mechanisms to protect against malware.”
4. The proposed VVSG 2.0 fails to define the threshold of harm and predictability that “harmful conditions” must meet in order to require *a priori* protection.
5. The proposed VVSG 2.0 fails to define how an election official would be able to identify “appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice,” and when it becomes necessary to update those defenses.
6. Particularly problematic are the recurring reliance on the words “current” or “currently” which don’t explain if they refer to the time of the adoption of VVSG 2.0, the time the system is first implemented, or the time each election is held.
7. The VVSG 2.0 fails to address, in its lists of specifics, terms that are in the headings such as “cast as intended.”
8. The VVSG 2.0 fails to define who will fill-out or interpret the glaring gaps in its language, how stakeholders can request such definitions or interpretations, and what guarantees of impartiality come with that delegated authority.
9. The current makeup of the VVSG 2.0 implies that there will be subsequent processes to define the gaps and details, but those are not spelled out and there are no guarantees regarding their content or the processes to comment on them. The vagueness of VVSG 2.0 points to upcoming drawn-out arguments regarding what the

document means to say in those subsequent processes instead of addressing the true concerns. This makes approval of VVSG 2.0 premature, at best, and a blank check at worst.

10. Beyond the Commission's current mandate, NHCSL plans to propose that ballot design standards be mandatory.

Thank you,

Guillermo L. Mena

Director of Legislation, Policy and Advocacy

NHCSL - The National Hispanic Caucus of State Legislators

Please note my new email: gmena@nhcsl.org

[444 N. Capitol St NW, Suite 404](#)

Washington, DC 20001

Office Phone: [REDACTED]

Cell Phone: [REDACTED]

www.nhcsl.org

This email may be protected by attorney-client privilege or other confidentiality laws. If you are not the intended recipient, I would appreciate that you inform me of the mistake and then please delete the email. An attorney-client relationship should not be presumed between us unless there is a signed contract to that effect, even in circumstances where the privilege may still apply.

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

Cliff Tatum <ctatum@eac.gov>

To: Guillermo Mena [REDACTED] >

Cc: "votingsystemguidelines@eac.gov" <votingsystemguidelines@eac.gov>

Fri, May 17, 2019 at 5:19 PM

Request received

[Quoted text hidden]

--

Clifford Tatum
General Counsel
301-563-3957

Confidential Notice: This message may contain Controlled Unclassified Information (CUI) that requires safeguarding or dissemination control under applicable law, regulation, or Government-wide policy. This email, including all attachments, may constitute a Federal record or other Government property that is intended only for the use of the individual or entity to which it is addressed. If you are not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify the sender by responding to the email and then immediately delete the email.



May 17, 2019

U.S. Election Assistance Commission

1st Floor Conference Room
1335 East West Highway
Silver Spring, MD 20910

Re: Written Testimony for Third Public Hearing on Voluntary Voting System Guidelines 2.0 Principles and Guidelines

The Voluntary Voting System Guidelines (VVSG) are critical to the promulgation of high-quality principles, specifications, and requirements that ensure the integrity of every vote cast by every voter, including voters with accessibility needs. The importance of regularly updating the VVSG to remain relevant to addressing the ever-evolving needs of voters and threats to voting systems cannot be understated. Given the broad range of topics covered by the principles, I would like to focus my testimony on Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS, Principle 6: VOTER PRIVACY, and Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE.

HAVA calls for voters to be able to vote privately and independently without assistance from others. For the millions of voters with visual, mobility, cognitive, and other disabilities (12% of 2016 General Election voters) that means relying on accommodations, often through digital technologies. Some of this digital technology can be used independently and securely by leveraging the voters' personal assistive technology. For example, an online voter registration website can be designed to provide an equivalent and consistent experience to a sighted voter without assistance and a non-sighted voter assisted by screen-reading and voice input technologies at home. Both experiences are secured using the same web-based security protocols implemented as part of the website's design. Ballot marking devices (BMD) at polling places have flexible capabilities such as adjustable text size, multilingual audio, and personal input device interfaces that allow voters with disabilities the opportunity to interact with the same ballot as other voters. The same devices benefit all voters because their flexible capabilities provide the opportunity for increased functionality such uniform ballot marking, prohibition of overvotes, and minimizing the conditions for coercion. Assistive technologies can address the concerns of multiple constituencies if they are designed, developed, and implemented with the guidance of thoughtful standards and requirements.

The foreign interference of the 2016 elections has sharpened the priority of local, state, and federal officials on the security of digital technologies used throughout election systems. Unfortunately, many of those components and systems were designed, developed, and implemented using the VVSG 1.0 and 1.1 that are no longer adequate to meet today's security concerns. Beyond physical security and cybersecurity, there is an increased expectation of accountability in the election process as a means of reducing the ability of interfering with votes and voters. Components and systems must face a higher standard of robustness, safety, and verifiability but not at the expense usability and accessibility.



CENTER FOR
DEMOCRACY
& TECHNOLOGY

Jurisdictions need to be able to look to VVSG 2.0 as they consider how their election models evolve to include vote-by-mail, electronic pollbooks, consolidated vote centers, and risk-limiting audits. All of those evolutions require substantial investments in digital technologies that should serve all voters regardless of their abilities and without discrimination..

Nearly every state relies on the VVSG for their state certification process, and consequently nearly every voter does as well. It is important that the EAC continues this open process of discussion and consideration to ensure that both security and accessibility concerns are addressed in design of voting components and systems so that every voter benefits from the enhancements in privacy and accessibility.

Sincerely,

A handwritten signature in black ink, appearing to read "M.T." or "Maurice Turner".

Maurice Turner, Senior Technologist

Aaron Wilson – VVSG 2.0 Comments

June 3, 2019

Please accept the following comments on the proposed structure and composition of the VVSG 2.0 Principles and Guidelines. The following are the personal comments of Aaron Wilson. These do not represent the views of the Center for Internet Security (CIS).

Comments on the proposed structure of Principles, Guidelines, Requirements, and Test Assertions and the proposed governance of these: commissioner level approval will be required to change Principles and Guidelines and staff will have authority to change Requirements and Test Assertions without commissioner approval.

On the structure itself, I support the construction of higher-level concepts which are broken down into more granular details. When it comes to product requirements – an area I have worked for over a decade – there is often a dividing line between higher-level goals and lower-level requirements and then a separate line between those requirements and detailed implementation tasks. Each type of product development artifact just mentioned – goal, requirement, and implementation task – has a different but complimentary purpose. Goals are typically agreeable and understandable to multiple audiences and are often used in initial conversations to frame the work. Goals are then decomposed into requirements by someone familiar with the products and technology. The best requirements don't dictate an implementation approach and are still mostly understandable to non-technical audiences. Finally, the implementers convert the requirements into detailed implementation tasks which are used for the actual development. Implementers are given flexibility in the implementation so long as they achieve the goals within the parameters set forth in the requirements. I mention this typical breakdown in product development artifacts because I believe it has applicability here.

- Goals – I believe the Principles and Guidelines are universally agreeable goals that set the framework for the requirements. The current Principles and guidelines are a great start; though, I do have some comments on their proposed composition. It is critical to get these right because you don't expect these to change often at all.
- Requirements – these are synonymous with the requirements for product development. We want requirements that are not implementation or technology specific and are still relatable to a broad audience. We want this for two reasons:
 1. We don't want to impose implementation approaches on voting system manufacturers. We want innovation and competition within a set of constraints established to ensure EAC certified voting systems are secure, reliable, and accessible. We want new companies to enter the market with new ideas; and we want differentiation in the market to give states and counties the ability to choose the product which is most appropriate for them.
 2. We don't want requirements to become outdated too quickly. A stable set of requirements which remain technologically relevant for a reasonable amount of time is the best possible outcome and should be the goal of the requirements creation process. It is possible – but not the most natural – to write detailed requirements without the bias of currently known technology. On the other hand, it is not reasonable to expect requirements to remain technologically relevant for more than a decade. Given the historical amount of change in the voting system technology space, a thoughtful requirements creation process which aims to write implementation agnostic

Aaron Wilson – VVSG 2.0 Comments

June 3, 2019

requirements should yield requirements which are technologically relevant for at least 8 years. Many people think the requirements will become outdated much quicker than 8 years, but that is based on a desire to write more technology-specific requirements. It is not clear if the current requirements developed through the NIST working group approach meets this 8-year-relevancy objective.

- Implementation Tasks – this is synonymous with the VVSG 2.0 Test Assertions. These should be implementation and technology specific. They should consider how the voting system is built to achieve the goals and requirements. When new and innovative approaches are presented to achieve the requirements, the test assertions need to adapt to appropriately test the technology against the requirements.

Given this information, I believe if the requirements are written appropriately, the commissioners should be capable of and are the appropriate authority to review the Principles, Guidelines, and Requirements. The Test Assertions and details on how the certification program is run (i.e. the certification process) should be in the purview of EAC staff. I have a couple additional comments to support this position:

- Under the current authority proposal and current proposed Principles and Guidelines, staff will have too much leeway to significantly alter the expected outcomes of the voting system program. The Principles and Guidelines are too vague and leave open the option for staff to create a much weaker or overbearing certification process. For example, guideline 2.4 reads “Voting system structure is modular, scalable, and robust”. The adjectives of modular, scalable, and robust can be used to defend nearly any requirement staff wanted to add.
- With the proposed governance, EAC staff will become the target of lobbying efforts by special interest groups who all have a stake in the VVSG requirements. Given the authority left to them by the vague nature of the Principles and Guidelines, staff will become the target of coordinated and motivated efforts to secure consequential changes to the requirements. This could be voting system vendors or other groups who have financial or ideological stakes. This would create an inappropriate situation and create additional burden for staff.

Comments on the text of the Principles

Principle 4 refers to “interfaces to internal components”. The format of internal voting system communication should not be governed by the VVSGs and the associated Common Data Formats (CDFs) being developed by NIST. The Common Data Formats are “common”, and, as such, are not optimized for specific implementations. Voting system vendors should be allowed to optimize the data formats they use internally. The optimization is necessary for scalability and performance reasons. Using the CDFs internally has the risk of limiting the voting system’s ability to operate most efficiently. Conversely, requiring CDFs for external interfaces makes perfect sense.

The word “robust” in principle 8 doesn’t have any meaning or guidelines around it. It sounds good but doesn’t have any definition. I would suggest removing it for clarity and brevity.

The wording of principle 14 stands out to me because it is not written like the others. It appears to be more succinctly stated as “The voting system functionality is protected against service outages and unauthorized manipulation, whether intentional or accidental.”

Aaron Wilson – VVSG 2.0 Comments

June 3, 2019

Comments on the text of the Guidelines

2.2 - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers.

The content of this guideline is fine, but the wording and structure could be improved. I suggest: “The voting system is implemented using best practices in user-centered design that consider a wide range of representative voters, including those with and without disabilities, and election workers.”

2.4 - Voting system structure is modular, scalable, and robust.

This is very nebulous and leaves a lot of room for requirements variation. What is meant by structure? Modular, scalable, and robust can become buzz words and their meanings twisted and used to support all sorts of requirements. There is no mention of performance, portability, and other attributes which you often see with these¹. Will the absence of some of these mean they are not required?

2.5 – The voting system supports system processes and data with integrity.

I am struggling to make sense of the concept of supporting processes and data “with integrity”. I think this sounds good but doesn’t have true meaning. There is also a principle on integrity. Is this different? Maybe a better wording is “The voting system implementation protects the integrity of system processes and data.”. I think this wording is clearer but still seems to duplicate the Principle 14: System Integrity.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

It seems like the word “comprehensive” should also be used to describe the documentation. Also, what does is meant to “be read”. I’d like to assume all documentation will be readable. Maybe consider changing to “...and other aspects of the voting system is comprehensive and understandable.”

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

While not intended, this guideline does not account for the voting system operations which should not be publicly verifiable. Most notably, the public should not be allowed to verify the act of individual voting for privacy reasons.

4.2 - Standard, publicly-available formats for other types of data are used, where available.

What is meant by “other types” here? I assume it is referring to types not mentioned in 4.1. If so, that should be stated specifically.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

I think this is self-explanatory. Shouldn’t any device be accepted if it meets the applicable VVSG requirements? Does calling out COTS unintentionally exclude other options?

5.1 - Voters have a consistent experience throughout the voting process in all modes of voting.

¹ See https://en.wikipedia.org/wiki/List_of_system_quality_attributes for examples of quality attributes.

Aaron Wilson – VVSG 2.0 Comments

June 3, 2019

I agree with the spirit of this guideline but there are practical limitations to this. Modes of voting can be very different, and some are outside the control of the voting system (i.e. postal voting). How can this guideline be fully enforced on a voting system? This same comment applies to 5.2. For example, how can the voting system provide an audio ballot option in all modes of voting?

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

I think what is meant by “ballot changes” in this guideline is control over the ballot marks, but the phrase “ballot changes” is very broad. I would suggest changing the end to “...have direct control over marking, verifying, and casting the ballot”.

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction. 8.4 The voting system is evaluated for usability by election workers.

These guidelines are too vague and do not state an expected outcome. This leaves a lot of room for the requirements and EAC staff to determine what is acceptable and not. I understand these are difficult quality attributes to measure, but I think the wording of the guidelines needs to try to set a reasonable bar.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

I don't believe this is the most appropriate wording. I think the phrase “modified as needed” is meant to refer to the access privileges but it almost reads like it is referring to the logs – which you don't want to modify. Additionally, it is difficult for the voting system to perform the monitoring and periodic reviewing of logs. You ideally want a person to do this. The wording should probably be changed to focus on the voting system enabling the periodic monitoring and reviewing of the logs. It should also enable modification of access privileges, which is currently also covered in Guideline 11.3.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

I don't believe “redundancy” is the best word here. Redundancy is a common tactic but not necessarily a goal. I think what fits better here is “resiliency”. Resilience can be accomplished by having multiple layers of controls as well as by redundancy of systems.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

I am concerned about how the word “report” may be interpreted here. I have concerns it may be interpreted as reporting to a user. It may not be possible, desirable, or necessary to report all error messages to a user as they occur. If “report” means log the error message, this is ok. This should be clarified.

15.3 - The voting system employs mechanisms to protect against malware. 15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

15.3 and 15.4 seem more appropriate under Principle 14. They don't seem to fit best under Principle 15: Detection and Monitoring.



May 29, 2019

VIA ELECTRONIC SUBMISSION

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Public Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

Thank you for the opportunity to comment on the draft Voluntary Voting System Guidelines (VVSG) 2.0. Principles and Guidelines.

Every year agencies such as Arizona Center for Disability Law (ACDL), the federally designated Protection and Advocacy (P&A) system for Arizona, utilizes HAVA funding to complete multiple projects that advocate for greater access to Arizona voting systems for people with disabilities. This includes projects such as poll-worker training covering topics like procedures regarding voters with disabilities, how to operate accessible voting equipment at polling sites, obligations regarding accommodations under Title II of the Americans with Disabilities Act and Arizona Civil Rights Act, and general disability etiquette.

Through the Protection and Advocacy for Voter Access (PAVA) program, created by the Help America Vote Act, the P&As have a federal mandate to *“ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places”* and are the leading expert on access to the vote for people with disabilities in the United States.

ACDL applauds the US Election Assistance Commission (EAC) for attempting the complex task of balancing election security with federal elections accessibility requirements under law. However, we are concerned that the only voting systems capable of meeting VVSG 2.0's requirements will be reliant on a marked paper ballot as the ballot of record. This concern that has been further confirmed by the technical standards for the VVSG that are currently being developed in public forums. The promise of a fully accessible, paper-based voting systems is as old as the passage of HAVA itself. Yet, the dream that paper ballots will be made accessible, private and able to be cast independently, for people with disabilities is not now, and may never be, a reality. Widespread implementation of market-ready, fully accessible paper ballot voting

5025 East Washington Street, Suite 202
Phoenix, Arizona 85034-7437
(602) 274-6287 (Voice) – (602) 274-6779 (Fax)

177 North Church Avenue, Suite 800
Tucson, Arizona 85701-1119
(520) 327-9547 (Voice) – (520) 884-0992 (Fax)

www.azdisabilitylaw.org

systems is simply not achievable within the near future.

Increasingly, voters with disabilities and their non-disabled peers are leveraging opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. Yet, VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the extent of the VVSG's reach into non-traditional voting systems. The failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated systems are a form of discrimination and **inherently unequal** and should no longer be considered a standard, acceptable practice in the United States.

The assumption that a majority of voters will hand mark their ballots means that there are a limited number of accessible voting machines present. Poll workers are insufficiently prepared to operate them. As a result, poll workers at their best are unable to describe and activate accessibility features included in the equipment's design. At worst, elections personnel discourage use of the equipment by voters or leave the voting machine turned off, still in its case, and even hidden from view.

America's elections must be accurate. The EAC must, in this process of a comprehensive re-envisioning of the guidelines, expand the VVSG's reach to encompass all technology used to cast ballots within or beyond the traditional polling place. The VVSG must ensure a private and independent ballot for all voters in a fully integrated experience that respects the dignity of the voter and the secrecy of the ballot.

Voting is a fundamental right, and there are state and federal laws that protect the rights of persons with disabilities in the voting process. The EAC must work with Arizona and all states in making the voting process safer and more accessible for all people, including those with disabilities.

Thank you for the opportunity to comment on this important set of principles and guidelines. If you have any questions please contact Natalie Luna Rose at nlunarose@azdisabilitylaw.org.

Sincerely,



J.J. Rico
CEO
Arizona Center for Disability Law



May 29, 2019

Submitted Electronically

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Re: Comments on EAC VVSG 2.0 of the U.S. Technology Policy Committee of the Association for Computing Machinery

Dear Chairwoman McCormick:

The Association for Computing Machinery (“ACM”) is the longest established and, with more than 100,000 global members, the largest association of individual professionals engaged in all aspects of computing in the world. A non-lobbying and otherwise wholly apolitical organization, ACM’s mission includes providing unbiased, expert technical advice to policy-makers on matters of our members’ wide-ranging expertise. That work is accomplished in the United States by and through ACM’s U.S. Technology Policy Committee (the “Committee”).

The Committee commends the Commission for opening this proceeding to refine the second iteration of its Voluntary Voting System Guidelines (“VVSG 2.0”) and, consistent with our mandate, is pleased to again¹ have the opportunity to assist the Election Assistance Commission. We look forward to future opportunities to comment in greater technical detail upon the means of implementing the high-level principles and guidelines that are currently (and we believe productively) the focus of this stage of the proceeding. For present purposes, the Committee wishes to:

¹ Committee member David Wagner leads the security team of the EAC’s Technical Guidelines Development Committee (TGDC) on which Committee member Ron Rivest and Vice Chair Jeremy Epstein also previously sat. Epstein also served as a panelist at the EAC’s January 10, 2018 Summit on the 2018 election.

- associate itself with select comments, detailed in the attached matrix, of several other respected civil society organizations,² as well as with specific points made in the individual filing of Dr. Philip Stark;
- clearly underscore that, to be as secure and verifiable as possible, *all* voting technology must be: ***isolatable*** from inherently vulnerable networks of all kinds; ***inspectable*** with very high confidence at every stage of operation; and ***interoperable*** to maximize efficiency and system modernity.

The Committee thus specifically and emphatically recommends that the final VVSG:

1. **Endorse a blanket ban on the internet connection capability of any and every voting technology addressed by the VVSG, *including connection to any private network that ultimately may connect to the internet*.** This categorical prohibition on the inclusion of any connectivity-enabling devices in election-related equipment include all wireless modems, radios, and any other type of equipment capable of communicating over the internet. *Simply disabling such devices if installed will not suffice to protect election networks, databases and equipment.*
2. **Foster and justify public confidence that our election results are wholly evidence-based by requiring that elections be fully and robustly auditable.** To accomplish this goal, *all post-election ballot audits must occur before results are finalized and certified.* Moreover, such universal post-election assessment must include both *compliance audits* that verify the audit trail and *risk-limiting* ballot audits that either validate the declared results or determine what the correct results should be.
3. **Require the full interoperability of all internal voting system components, peripherals and data formats, together with component and system integration testing and certification.** Component testing would significantly decrease vendor development and testing costs. Component certification, combined with interoperability, almost certainly would decrease the costs and increase the options of election officials by facilitating the modular replacement of only those portions of their systems that require upgrading rather than systems in their entirety, as is now the norm. Component testing also would lower the barriers to market entry for new and potentially innovative component-producing companies which would be relieved from the present burdens of having to develop complete election systems.

² The Committee has carefully reviewed and emphasizes in the attached Appendix select observations and recommendations of the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), and Verified Voting (VV).

Thank you again for the opportunity to participate in this critical effort. Should you or your staff have any questions regarding these Comments, or seek further expert analysis or information our members may provide, please email Adam Eisgrau, ACM's Washington-based Director of Global Policy & Public Affairs, at the address below or reach him at 202-580-6555.

Sincerely,



James A. Hendler, Chair

Appendix

Appendix

ASSOCIATION FOR COMPUTING MACHINERY U.S. TECHNOLOGY POLICY COMMITTEE COMMENTS ON EAC VVSG 2.0 ADDITIONAL CONCEPTS AND COMMENTS ENDORSED

ACM's U.S. Technology Policy Committee also makes the following additional general points (*unattributed*) and associates itself with the specific analyses of VVSG 2.0 identified below articulated variously in their Comments by: the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), Verified Voting (VV), and Dr. Philip Stark (PS).

Principle	Issue	Comment/Analysis	Source(s)
General	Structure	■ Separation of proposed principles from detailed technical requirements.	PS
General	Process	■ Approval of technical requirements and test assertions without EAC vote.	VV
General	Objective	■ VVSG must: "deliver meaningful and effective guidance and requirements that will improve the security of voting systems and lessen exposure to manipulation, tampering or hacking."	NEDC
General	Auditability	■ Our nation must conduct and verify fully auditable evidence-based elections.	PS, SAWG, VV
General	Connectivity	■ No device involved in balloting or election administration should be connected or connectable to the internet or any private network that connects to the internet.	EPIC, NEDC, PS
4	Interoperability	■ Strongly supported for all devices and data.	
5	Voter Access	■ Voters must have equal and consistent access to election systems and resources.	
6	Voter Privacy	■ Voter privacy must be assured and protected in all phases of the election process.	
7	Ballotting	■ Ballot text, form and vote selections must be presented in a clear and understandable way that can easily be marked and verified by all voters. ■ Voting systems must allow voters to consistently and accurately verify both their ballots and the auditable records of their votes. ■ Voters with disabilities must be able to independently validate their ballots.	VV PS

8	Voting Systems/ Processes	<ul style="list-style-type: none"> ▪ Voting systems and processes must be “robust, safe, usable and accessible. ▪ 8.3: System accuracy and ease of use must be prioritized over voter “satisfaction.” 	PS VV
9	Auditability	<ul style="list-style-type: none"> ▪ 9.2: Election/voting records must be verifiable by the voter. 	VV
10	Ballot Secrecy	<ul style="list-style-type: none"> ▪ It should not be possible to link the voter to his or her ballot once the ballot has been cast. ▪ “Voters should vote privately . . . but votes should [more accurately] be [considered and described as] anonymous rather than secret.” ▪ Delete “recallable ballot” from the glossary as the notion of a recallable ballot inherently conflicts with a ballot secret and anonymity. 	EPIC PS SAWG
13	Data Protection	<ul style="list-style-type: none"> ▪ Add a separate guideline articulating the clear prohibition on internet “connectivity,” above. 	NEDC
15	Detection and Monitoring	<ul style="list-style-type: none"> ▪ 15.4: As this provision presumes the interconnection of voting systems with the internet or other networks in contravention of the recommended prohibition, it should be eliminated. 	PS
Glossary		<p>The Committee also concurs that the following key Glossary terms should be added or modified:</p> <ul style="list-style-type: none"> ▪ Audit ▪ Ballot ▪ Ballot Secrecy ▪ Ballot Selections ▪ Cast Vote Record ▪ Correct (re: election outcomes) ▪ Effectiveness ▪ Efficiency ▪ Resilience ▪ Sensitive Data ▪ Voter Selections 	PS PS, VV SAWG, VV SAWG PS, SAWG, VV VV PS PS SAWG VV SAWG

To: U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

From: Aquene Freechild
Secure Our Vote Coalition & Public Citizen
c/o 1600 20th St. NW
Washington, DC 20009

Re: Comments on the VVSG 2.0 Principles and Guidelines

Dear Chair Christine McCormick, Vice-Chair Benjamin Hovland, Commissioner Thomas Hicks, Commissioner Donald Palmer and the staff of Elections Assistance Commission (EAC),

Please find contained in this package individual comments received by the Secure Our Vote Coalition, DailyKos and Public Citizen. These comments are in support of passage of stronger VVSG 2.0 Principles and Guidelines that make clear that voting systems with wireless capability are not secure and should not be certifiable.

These comments were submitted directly to the email address provided by the EAC on the Federal Register as well.

The comments in this package number approximately 669 individual comments in support of banning wireless from VVSG certified voting equipment.

We will provide an electronic file with the comments as well to make it easier for you to process the unique comments.

Thank you for your consideration.

Sincerely,

Aquene Freechild

On behalf of the Secure Our Vote Coalition & Public Citizen

			<p>WE 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. Thank you for your consideration of this update to the latest set of guidelines.</p>
John and Ro: Martin		2019-05-29 19:20:31	[REDACTED]
Matthew Munsey	eac-comments@n	2019-05-29 22:49:55	<p>I applaud the EAC moving forward the latest Voluntary Voting System Guidelines, especially protections for software independence and auditability of elections. In addition to other safeguards, it only makes sense to prohibit wireless or other networking hardware in machines involved with counting or tabulating votes. Such capabilities only increase opportunities for cyberattack or manipulation, and software cannot adequately prevent such hardware from being enabled by malicious actors or programming errors. 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.' Eliminating wireless modems and networking capabilities cannot prevent manipulation through other means, which 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. Thank you for your consideration of this update to the latest set of guidelines.</p>
Jeff Rose		2019-05-30 00:19:47	<p>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. Thank you for your consideration of this update to the latest set of guidelines, and please protect our votes! Sincerely, Mr. Jeff Rose Oakland, CA 94602</p>
Bayard Taylor		2019-05-30 04:26:35	<p>Our democracy depends upon reliable elections. But computerized voting systems that connect to the internet and that do not include paper ballots for back-up counting invite corruption. We must do this even if it were not the case -- which it is -- that our elections are being interfered with with cyber attacks. Therefore, we must support the draft Voluntary Voting System Guidelines (VVSG).</p>

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. Thank you for your consideration of this update to the latest set of guidelines. Just use paper ballots

Travis Golison [REDACTED] cc GMT 2019-05-30 08:08:02

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. Thank you for your consideration of this update to the latest set of guidelines. I am an election judge and we need to make every voice count. Protect equipment and give a written conformation of each vote to check to be sure that nothing was changed or cancelled out. This is so important

Mary Lawless [REDACTED] r GMT 2019-05-30 16:37:29

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 actively 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.' 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. Thank you for your consideration of this update to the latest set of guidelines.

ROBIN GOODPAST [REDACTED] GMT 2019-05-31 21:12:10

- I support the draft Voluntary Voting System Guidelines (VVSG) and commend the robust principles and guidelines for software independence, ability to audit the voting process, and ballot secrecy. 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 must ban modems in vote counting machines to protect data and prevent manipulation. The Commission must 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.
- Susan Westervelt [REDACTED] 2019-05-31 21:25:55 GMT Thank you.
- 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. Thank you for your consideration of this update
- Kathleen Wallace [REDACTED] 2019-05-31 23:50:22 GMT to the latest set of guidelines. Democracy is falling through our fingers like water.
- We must protect the integrity of our elections across the US. 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. Thank you for your consideration of this update to the latest set of guidelines.
- Maradel Gale [REDACTED] 2019-06-01 00:27:48 GMT

Mary Stewart [REDACTED] GMT

2019-06-01 22:59:25 I strongly support the draft Voluntary Voting System Guidelines (VVSG) and commend the robust principles and guidelines for software independence, auditability and ballot secrecy. We need to protect our elections if we are to continue as an independent nation. This should not be a partisan matter. It is much more important than that. 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. Thank you for your consideration of this update to the latest set of guidelines.

Mark McKennon [REDACTED] GMT

2019-06-02 19:32:09 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. If you want to do the same, you should create a system that is much more reliable. How much will that cost? Well, how much will a failing system cost?: a further loss of faith in government, for thing. That would be unaffordable and unacceptable. 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. Thank you for your consideration of this update to the latest set of guidelines.

			Please, Do the Right Thing for Ours and Our Children's Future. What would They be Proud Of? 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. Thank you for your consideration of this update to the latest set of guidelines.
Milan	Mehta	2019-06-02 20:58:53	GMT
Jorgen	Harmse	2019-06-02 21:57:19	GMT
Kathleen	Eichinger	2019-06-03 01:09:04	GMT

Tom

Bruno

[REDACTED]

2019-06-
03
22:14:16
GMT

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. I would also like to see a prohibition of the use of barcodes to tally votes, especially in machines that feed the completed ballots back in front of the print heads AFTER reviewing it and hitting the submit button. Voters need to know that the bar code is not getting smudged or rewritten before the count and the subsequent storage. Thank you for your consideration of this update to the latest set of guidelines.

Jim&Betty BURRELL

[REDACTED]

2019-06-
04
01:06:19
GMT

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. Thank you for your consideration of this update to the latest set of guidelines.

May 23, 2019

Commissioner Christy McCormick
Chairwoman
United States Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, Maryland 20910

Submitted electronically via www.regulations.gov

Re: Comments from the Bipartisan Policy Center on EAC's Proposed "Voluntary Voting System Guidelines 2.0 Principles and Guidelines" (Docket ID No. EAC_FRDOC_0001)

Dear Chairwoman McCormick:

The Bipartisan Policy Center is a nonprofit organization that combines the best ideas from both parties to promote health, security, and opportunity for all Americans. BPC drives principled and politically viable policy solutions through the power of rigorous analysis, painstaking negotiation, and aggressive advocacy. Our policy solutions are the product of informed deliberations by current and former elected and appointed officials, business and labor leaders, and academics and advocates who represent views from across the political spectrum.

BPC is pleased to submit comments on the U.S. Election Assistance Commission's proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines. BPC's Elections Project builds on the success of our efforts to enhance the voting experience by implementing the recommendations of the Presidential Commission on Election Administration. The Elections Project has convened three task forces in 2019 to analyze voting in America, develop bipartisan recommendations that improve the voting experience, and engage in the 2020 election conversation with respect to registering to vote, casting a ballot, and counting the vote. The Elections Project maintains relationships with local and state election administrators and policymakers and administers the largest data collection of line lengths at individual polling places throughout the country.

The proposed standards are the result of years of work by experts, administrators, and policymakers throughout the government, nonprofit, and advocacy sectors. All should be commended for their dedication to America's voters.

Voters expect and deserve voting systems 1) on which they can make and change selections in an accessible, private, and independent manner with safeguards against inadvertent invalidation of their results, and 2) that produce an auditable record.

The proposed structure of the new VVSG as principles and guidelines for EAC commissioner adoption—along with separate technical requirements and test lab assertions that do not require commissioner adoption—will result in the development of voting technology that meets

federal standards and improves the voting experience without the additional risk of partisan or quorum concerns.

The EAC seeks feedback regarding all sections of the Voluntary Voting System Guidelines 2.0 Principles and Guidelines including the proposed structure of VVSG 2.0. BPC supports all 15 high-level principles as essential components of a voting system that works for the voter and increases confidence in end results. We have no comment on the specific principles and guidelines proposed.

Our comment, therefore, focuses on the new structure for VVSG 2.0. We support this new structure for three reasons:

1. The local and state election administrator community strongly endorses a structure for VVSG 2.0 that separates out the principles and guidelines from the technical requirements and voting system testing lab assertions. In fact, the National Association of State Election Directors (NASED) VVSG committee should be credited with proposing the new structure for the Voluntary Voting System Guidelines, as that group started focus on these changes more than five years ago. The EAC's own Board of Advisors and Standards Board endorsed the structure. Those two boards include nearly 150 local, state, and national experts representing every state in the country and numerous interests identified by Congress during the drafting of the Help America Vote Act of 2002. The Technical Guidelines Development Committee has also endorsed this new structure. These boards are meant to provide EAC commissioners a real-time assessment of the election official and advocacy community as EAC works to further its mission to help election officials improve the administration of elections and Americans participate in the voting process. They are intent on creating consistent, implementable guidelines for which technical requirements and testing lab assertions can be updated in short order by voting system technical experts as technology evolves.
2. While there is a full complement of commissioners now serving on at the EAC, that is not always the case, and BPC cannot endorse a structure of VVSG 2.0 that is inflexible should quorum issues reemerge at some point in the future. We expect the principles and guidelines to require review every few years while the technical requirements and voting system testing lab assertions may need more regular updating as new technology is invented and enters the market.

Based on a [BPC analysis from December 2018](#), the EAC has had all four commissioner slots filled simultaneously for less than a third of its time in existence. Between the beginning of 2012 and the end of 2018, there was an operational quorum of three commissioners less than half the time. The EAC's lapse in maintaining current, state-of-the-art guidelines can be traced directly to its quorum issues. This fact undermines Americans' confidence in the voting systems when they hear the systems in use today are built on guidelines that were mostly written more than a decade ago.

3. The structure of the EAC as strictly bipartisan was smart and the vast majority of EAC actions have been adopted unanimously. Election policy should be endorsed by Republicans and Democrats together through the political appointees on the EAC.

However, one needs only to look at the U.S. Federal Election Commission to see that partisanship can hamstring a bipartisan agency. While the principles and guidelines of the voluntary voting system guidelines are a policy level consideration appropriate for the commissioners' attention, the technical requirements and voting system testing lab assertions are procedural documents that do not implicate policy concerns and should not be subject to future partisan disagreement.

Voting system experts at the National Institute of Standards and Technology (NIST) and on the EAC staff need flexibility in maintaining and evolving the technical requirements and voting system testing lab assertions to ensure Americans regain and keep confidence that the voting technology is free from partisanship.

A new structure of VVSG 2.0 that codifies sub-commissioner level changes to the technical requirements and voting system test lab assertions could also allow for a policy change by which the full commission becomes the appeals panel to any NIST and EAC staff decisions to update the technical requirements and voting system test lab assertions. However, any such policy should be structured in a way that allows the process to move forward until a commission vote is taken that overturns a NIST and EAC staff decision. This structure maintains a strong and important role for the commissioners in overseeing the testing and certification of voting systems in situations where policy-level concerns may arise while avoiding the aforementioned quorum issues that have halted the process in the past.

In conclusion, BPC strongly believes that the new structure of VVSG 2.0 is better for election officials, vendors, and, most importantly, American voters. BPC encourages the EAC to consider these comments as it endeavors to create voluntary voting system guidelines that reflect modern technological advancement and that work in today's political environment.

Sincerely,

Matthew Weil
Director, Elections Project
Bipartisan Policy Center



May 29, 2019

U.S. Election Assistance Commission

Voluntary Voting System Guidelines 2.0. Principles and Guidelines Comments

1335 East West Highway
Silver Spring, MD 20910

Re: Voluntary Voting System Guidelines 2.0. Principles and Guidelines Comments

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 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.¹ 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.² 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 29147/30111³). The testing and certification process should confirm that each manufacturer 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.⁴ 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

¹ 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-e slate-voting-ballot-switch-problems>.

² 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.

³ 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>.

⁴ 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>.



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 collaborators⁵ 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 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 the database.⁶

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,⁷ 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

⁵ See: <https://github.com/usnistgov/ElectionEventLogging>.

⁶ 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>.

⁷ 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>.



communication, notably, the HTTPS standard.⁸ 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.
7. **Accessibility:** Millions of voters with visual, mobility, cognitive, and other disabilities (12% of 2016 General Election voters)⁹ rely on accommodations, often through digital technologies. Some of this digital technology can be used independently and securely by leveraging the voters' personal assistive technology. For example, an online voter registration website can be designed to provide an equivalent and consistent experience to a sighted voter without assistance and a non-sighted voter assisted by screen-reading and voice input technologies at home. Both experiences are secured using the same web-based security protocols implemented as part of the website's design. Ballot marking devices (BMD) at polling places have flexible capabilities such as adjustable text size, multilingual audio, and personal input device interfaces that allow voters with disabilities the opportunity to interact with the same ballot as other voters. The same devices benefit all voters because their flexible capabilities provide the opportunity for increased functionality such as uniform ballot marking, prohibition of overvotes, and minimizing the conditions for coercion. Assistive technologies can address the concerns of multiple constituencies if they are designed, developed, and implemented with the guidance of thoughtful standards and requirements that prioritize equity.
8. **Add Additional Principle:** The definition of voting system in HAVA Sec. 301 (b) should be expanded to include systems, components, and services such as electronic pollbooks and cloud-based election night reporting websites that are currently outside the scope of EAC testing and certification. Products that are currently under development or not yet conceived may play a critical role in future elections and should undergo the scrutiny of testing and certification to

⁸ 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/>.

⁹ Lisa Schur and Douglas Kruse, *Fact sheet: Disability and Voter Turnout in the 2016 Elections*, (2016), available at: https://smlr.rutgers.edu/sites/default/files/documents/PressReleases/kruse_and_schur_-_2016_disability_turnout.pdf.



ensure that they do not become potential operational liabilities or vectors for malicious interference.

16: VOTING SYSTEM AND COMPONENTS DEFINITION

The voting system is defined to include the hardware, software, and services components necessary to conduct an election.

- 16.1 – The voting system includes components to register voters.
- 16.2 – The voting system includes components to prepare and cast ballots.
- 16.3 – The voting system includes components to tabulate, record, and transmit results.
- 16.4 – The voting system includes components to audit results.

Sincerely,

A handwritten signature in black ink, appearing to read "JLH".

Joseph Lorenzo Hall, PhD
Chief Technologist, CDT

A handwritten signature in black ink, appearing to read "M.T".

Maurice Turner
Senior Technologist, CDT

Date: **June 5, 2019**
From: **Chris Curto, WatchTheVoteUSA.com**
To: **The U.S. Election Assistance Commission**
Regarding: **VVSG 2.0 and Necessary Criteria to Ensure that Elections are Secure, Transparent, Accurate, and Verifiable.**
Enclosed: **One DVD-R Disk**

Dear Commission Members,

I have been involved in the election transparency movement since 2011, and have had the privilege of working with and learning from some of the premier election transparency activists in the country. I believe we have a very good understanding of how to ensure secure, honest, accurate, transparent, publicly verified elections.

The new voting system guidelines in the VVSG 2.0 are a good improvement over current guidelines, however, VVSG 2.0 does not adequately address security, transparency, or the ability of the public to verify that all votes are counted as cast.

It also relies on input from election equipment and software vendors, which is an obvious and critical conflict of interest.

I agree wholeheartedly with the recommendations presented by **SmartElections.US** (which you may already be aware of). They have done an outstanding job. However, a few other important recommendations must be added.

Below is the SmartElections.US list of criteria, followed by my additional recommendations. Following that is a link to the **comprehensive report submitted to the Presidential Advisory Commission on Election Integrity**, by WatchTheVoteUSA.com, just before the commission was disbanded. (The full report is also on the enclosed DVD-R.)

SmartElections.US criteria:

NO APPROVED VOTING SYSTEM WILL:

1. ... record votes directly to a computer memory without the voter reviewing a paper ballot.
2. ... have a modem or allow remote access.
3. ... allow the technical opportunity for a machine to change a ballot after the voter has cast it – even if the machine is under the control of malware.
4. ... be a hybrid machine – with a printer and a scanner in the same path.
5. ... encode votes using barcodes, QR codes, or any other format that is not verifiable by a voter without assistive technology.
6. ... allow weighted election functions that use decimal counting methods. Votes must be counted as whole numbers.

ALL APPROVED VOTING SYSTEMS WILL:

7. ... allow for the use of hand-marked paper ballots - not just a paper trail created by a machine, except for accommodations made for voters with disabilities.
 8. ... use durable paper, not thermal paper.
 9. ... support the ability to have an accurate hand-counted audit.
 - 10.... create a digital ballot image that is identical to the paper ballot.
- The EAC must create a panel of election security experts made of academics and technical experts with no relationship to vendors and no vested interest in emerging systems. The EAC needs to take input on the VVSG 2.0 from this panel - and other non-vested security experts on an ongoing basis.
 - The EAC must stop consulting vendors and their representatives for technical guidance. This is a conflict of interest, is unethical and is preventing security improvements from being implemented.

Additional recommendations:

All machines used must be able to accommodate independently made paper ballots with serial numbers (which are distributed to voters in true random fashion to ensure the secrecy of their vote).

All machines used must provide storage of ballot images, to provide easy access to such images AT THE PRECINCT POLLING PLACES for comparison to the actual ballots, for authentication by precinct election judges, BEFORE the ballots leave the public sight, with a view to those authenticated twin ballot images being immediately made available to the public for scrutiny.

Also, hybrid voting systems that combine a ballot-marking device, printer and scanner functions must be banned. These machines have the ability to add fake votes to paper ballots and steal elections without detection. Election security experts are calling these systems a "disaster."

Our elections **MUST** be honest, transparent, and publicly verified.

Other than removing all computers and machines from the voting and vote tabulating processes, the above recommendations provide the best chance for secure, honest, transparent, publicly verifiable elections.

Also, please read the WatchTheVoteUSA Report to the Presidential Advisory Commission on Election Integrity:

<http://www.watchthevoteusa.com/wtv-report-to-paci/>

Thank you in advance for your careful consideration of these important recommendations, and for your dedication to ensuring secure, honest, accurate, transparent, publicly verified elections.

Sincerely,



Chris Curto, WatchTheVoteUSA.com

Citizens' Oversight Projects (COPs)

771 Jamacha Rd #148
El Cajon, CA 92019
CitizensOversight.org
619-820-5321

June 3, 2019



U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Submitted via website form at <https://www.eac.gov/VVSG-form/>

COMMENTS ON VVSG 2.0 DRAFT

Thank you for this opportunity to provide comments on the Voluntary Voting System Guidelines, 2.0 document¹ during the extended time period for comments.

Introduction

Trained as an electronics and software engineer, I (and others associated with Citizens' Oversight) took an interest in election processing in about 2006. Between 2008 and 2010, we conducted an extensive in-depth review of the procedures used in San Diego County. This resulted in the development of audit oversight procedures which were implemented throughout CA and in other states, such as Florida, where audits are required by statute. We also provided oversight in the 2016 recounts, most particularly in Michigan. Since then, we have been working with other technical contributors to help to define improved election audits. Most recently, we have been developing Monte Carlo simulations to empirically understand how various type of audits will roll out so as to provide guidance to elections officials and citizens providing audit oversight.

Our point of view is primarily regarding how citizens can provide thorough oversight of elections. With sufficient public oversight, it will be impossible for extensive machine errors or hacking of the results to compromise our democracy.

General Opinion

We OPPOSE the adoption of VVSG 2.0 in its current form.

1. The Text of VVSG 2.0 at this stage is only 5 pages of extremely high-level statements that do almost nothing to provide technical guidance. We understand the impetus of taking this direction was to make it easier to adapt the guidelines as time progresses, so that only very high level statements approved as EAC voluntary guidelines can hopefully remain unchanged, while the Requirements and Test Assertions to be defined at a lower level, perhaps changing much more rapidly than the higher-level requirements. We reject the notion that a public process is inappropriate for the lower-level requirements.

1 https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

The document "VVSG Version 2.0: Scope and Structure"² states that "All previous versions of the VVSG provided device specific guidelines and requirements. The VVSG Version 2.0 will refrain from providing device-specific guidance and instead provide guidelines on the functions that are performed within those devices." (underlining added)

As a result, VVSG 2.0 provides very little guidance except that certainly everything should be of high quality, implemented with best practices, etc, sometimes using poorly defined and even conflicting terminology.

2. VVSG does not actually address the "functions that are performed" but instead talk of attributes of almost any function. "High Quality Design" is not function specific. Neither is "High Quality Implementation," "Transparent," etc. Certainly, there is not much disagreement on these highest-level goals, but to approve just these goals, and then trumpet perhaps that "The EAC has approved a new set of comprehensive guidelines" make it appear that a lot more has happened than is the case, and probably is counter-productive. Also, if manufacturers can similarly say "compliant with VVSG 2.0," this also provides almost no information.

3. Since the HAVA was initially adopted, the election integrity community has learned a great deal about the failings of the equipment and methodologies for voting and counting the vote. The initial systems were largely impossible to audit and would be easy to hack, as there was no "paper audit trail" and the vote could be changed internally without any external change that could be tracked. Ronald L. Rivest and John P. Wack published the document *On the notion of "software-independence" in voting systems* in 2008³ in recognition of this serious defect. Some touch-screen systems were adapted to include a printer "VVPAT" (Voter Verifiable Paper Audit Trail) device to fill this gap, but still many systems do not include such a device. To achieve software independence and maximize the likelihood that voters will verify their vote, it is extremely important that the voter see and verify their vote in the same durable and indelible record that will be used for the tabulation and any future audit. This typically means hand-marked paper ballots. Furthermore, many districts now find that Vote-by-mail (VBM) is either extremely dominant (more than 60%) or nearly 100% in many states (OR, WA, CO, etc). For this reason, the term "voting system" should include paper ballot and marking device. These are not electronic, but they are still *devices* that should be within the scope of the VVSG process.

The Election Assistance Commission seems to completely ignore this reality. Paper ballots are not considered a "voting system" because such things "must be electronic." We disagree with this silly restriction on what is included in the VVSG.

Indeed, such paper ballots are typically processed by central or distributed scanners and their format and layout is extremely important. Voting using hand-marked paper ballots is currently the best way to have voters both vote and verify that their vote has been recorded properly. They are also sufficient in any robust auditing process, so that the same record that the voter verified can be reviewed in the audit process.

Weaknesses in the current text

The current text was intended to be statements at a very high level so that hopefully no one can disagree. The trouble here is that they actually don't say very much. Nevertheless, in this section, weaknesses are listed.

1. In general, we believe that these high-level principles should be accompanied with at least a

2 [https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure\(DRAFTv_8\).pdf](https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf)

3 *On the notion of 'software independence' in voting systems*. Ronald L. Rivest. Philosophical Transactions of The Royal Society A 366,1881 (2008) pp. 3759--3767.

paragraph going into more detail about each one.

2. The guidelines should probably be separated into two functional categories, a) voter-facing devices at the polling place and b) vote counting equipment associated with Vote-by-mail and hand-marked paper ballots that are centrally processed.
3. The high-level goals may sound good, but are filled with "quishy" terms like "The voting system is designed using *commonly-accepted* election process specifications." Like what? Isn't this precisely the purpose of the "system guidelines"? Perhaps in an explanatory paragraph, examples of the commonly-accepted election process specifications can be included.
4. The VVSG has as a goal (Item 1.2) that the voting system should be "designed to function correctly." Really, we need to specify that as a goal? The problem is not that we want it to function correctly, but what does "correctly" really mean? This is not defined and so there can be a difference of opinion about what is correct.
5. Provision 1.3 says "Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not." Maybe it would be easier to just say "Voting system design supports testing of specified properties." I would suggest that this should go on to say that "any computer-based system will conduct internal consistency tests automatically and will expose intermediate data to allow function testing."
6. The term "best practice" is used numerous times. Best practice in whose opinion? Again, this is like saying nothing. Goals that use this may as well be not included at all. Best Practices in software development means design processes should be documented with review and feedback to improve the design process with lessons learned. Note: The "Capability Maturity Model" (CMM) is a development model created after a study of data collected from organizations that contracted with the U.S. Dept of Defense, who funded the research. The term "maturity" relates to the degree of formality and optimization of processes, from ad hoc processes to formally defined steps, to managed result metrics, to active optimization of the process.⁴
7. Item 2.2 "The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers" is really only applicable to voter-facing equipment. Again, these should be separated into separate functional groups, for voter-facing vs. central counting equipment.
8. Items 2.3, 2.4, are encompassed by 2.1. These are all best practices.
9. Item 2.5, "The voting system supports system processes and data with integrity." I believe this is a completely meaningless statement. What does "support" mean and what does "with integrity" mean? Suggest this should be deleted.
10. Item 2.6, it might be better to define what "handling errors robustly" actually means in more detail. Does it mean that all errors are logged? Does it mean the system must be fault-tolerant, implying a redundant multiple processor system that includes internal voting on every decision, such as is employed by truly fault tolerant systems? It probably does not mean to go that far, but it is simply unclear.
11. Item 2.7, it appears this is a redundant repeat of item 1.2. What is the difference between "1.2 - The voting system is designed to function correctly under real-world operating conditions" and "2.7 - The voting system performs reliably in anticipated physical environments." Is not "function correctly" also "reliable"?? Delete one of these, but again, it may be fine to delete both of them as they add nothing.

4 https://en.wikipedia.org/wiki/Capability_Maturity_Model

12. Item 3.1, this is one of the most important provisions as we found in our review of election procedures that they were poorly documented or not at all. Probably it is sufficient to say it is documented as it is difficult to assess whether something can be understood. And of course, it is implied that documentation "can be read." I suggest this change: "The voting system design, operation, accessibility features, security measures, and other aspects of the voting system are clearly documented."
13. Item 3.3: It is meaningless to have a goal that someone can understand something. Verify is sufficient. I suggest: "The public can verify the operations of the voting system throughout the entirety of the election."
14. Item 4.1 and 4.2 can be combined. These are also partly also important to Transparency. I suggest: "Voting system data that is imported, exported, or otherwise reported, is in an interoperable format defined by a public standard or as a widely used de-facto standard."
15. Suggest 4.2 be changed to: "data formats shall be human readable whenever possible." This again is related to Transparency.
16. On accessibility, these goals are nearly impossible to meet. "All voters can access and use the voting system regardless of their abilities, without discrimination." Although I support the notion, is it really possible to fulfill? What if a person is mentally incapacitated or perhaps lacking of all senses? Here, I believe there is nothing inherently wrong with having a certified pair of assistants help voters to complete their ballots rather than putting more trust in electronic systems. The set of requirements necessitated by very few voters who may not be able to use a hand-marked paper ballot independently have pushed the voting equipment toward very difficult-to-secure electronic systems that supposedly allow those voters to vote and verify their vote using assistive means. In reality, any reliance on such software or electronics means that those voters will in fact not be able to independently verify their vote. For example, if a blind voter relies on assistive gear to read back what is on the ballot, that system could read it properly while still submitting the vote differently. The only way to confirm that it was recorded correctly would be again to have two people to verify the ballot as it was recorded, such as on a paper ballot, and let the voter know what it says. That means we are back to having certified helpers for any voter who needs it. This is, we believe, a better solution than mandating expensive assistive technology. The "bring your own device" BYOD approach may be a better solution to avoid rarely used assistive devices at every polling place.
17. 5.1 and 5.2 are redundant. If voters have a "consistent experience" they will also "receive equivalent information." Very easy to combine these into a single provision. But what are "all modes of operation?" What is a mode? Not defined.
18. Principle 6 (Voter Privacy) and Principle 10 (Ballot Secrecy) should be combined and clarified. The term "ballot anonymity" should be used instead of Ballot Secrecy. Ballot anonymity means that the content of the ballots should be open and not secret while the linkage to the voter cannot be determined. During the voting process, each voter is thoroughly identified and validated as a qualified voter. The voting process itself is only optionally private. It is now commonly the case that many voters complete VBM ballots that are not necessarily completed in complete privacy, but each voter could isolate themselves and vote in private and then mail in the ballot in theory. It is now legal in many states (like CA) for voters to take selfies of themselves and their voted ballot.
19. Item 6.2, delete the phrase "or other associated cast vote record." Again, we believe it is not an inappropriate solution to provide certified assistants for voters who need help to vote and verify their selections if they cannot do it alone rather than instituting requirements that the voting system

must provide that accessibility.

20. Principle 7 is largely only appropriate for voter-facing electronic devices. However, similar provisions would also be appropriate for the layout and instructions on paper ballots, yet these are not included in the scope, which we believe is an inappropriate limitation of scope.
21. Statements like 7.3 "Voters can understand all information as it is presented, including instructions, messages from the system, and error messages." Sure, we don't want cryptic messages, but how can you prove that "voters can understand" something? Better written as follows: "All information presented to the voter, including instructions, messages from the system, and error messages, is presented in the language appropriate for the voter."
22. Item 8.1 is unclear, that "The voting system's hardware and accessories protect users from harmful conditions."? In what way? Does that mean that hand-marked paper ballots that do not "protect" voters from over-voting or spoiling a ballot are not supported? And what are "harmful" conditions"? Does that mean sharp edges or legs that will fold up without pinching fingers? Does it mean the voting system will protect voters if a mass-shooter should arrive on the scene? That's a pretty harmful condition, but hardly what this probably is intended to address. Listing examples of harmful conditions may be enough to clarify the meaning of this provision.
23. The term "currently" is very difficult, such as in "8.2 - The voting system meets currently accepted federal standards for accessibility." Does that mean current when this is approved, or current when the manufacturer designs it? Or current when users use it? What standards, like ADA? Much too hard to know so that it becomes impossible to apply.
24. Item 8.3 - "The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction." Does this just mean the size of the equipment is measured against the size of the voters, or would it be better to say "evaluated for usability" in the same way that is used in item 8.4? We think the latter would be better because the size is certainly a part of usability.
25. Item 9.1 - This is almost the definition of "software independence" mentioned earlier, but not exactly. It currently says "An error or fault in the voting system software or hardware cannot cause an undetectable change in election results." This should be expanded to include not just errors or faults, but malicious hacking. Thus, it should be: "An error or fault in the voting system software or hardware or malicious hacking cannot cause an undetectable change in election results."
26. Item 9.2 - Add "Records should be frozen in human-readable and machine processable formats that break down the results of the election to the smallest unit used in any comparison audit prior to performing any statistical selection procedure."
27. Item 9.4 - "The voting system supports efficient audits." This should not imply that the voting system itself is used to conduct audits, as such audits should not use software in common with the voting system. However, it is necessary to get reports from the election system that have sufficient granularity to check them against audited paper records. Here the "voting system" is more likely the election management system and central count software rather than voter-facing electronics.
28. Principle 10 -- This should be merged with Principle 6 as already mentioned. Ballot secrecy should be changed to ballot anonymity. Item 10.2 is good, however. This is essentially the definition of ballot anonymity.
29. Principle 11 -- Access control. This should be extended to state that voter-facing equipment should not be accessible on any public networks.
30. We have the implied notion that these voting systems will transmit data (13.1) and over "all

networks": 13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks, and 15.4 "A voting system with networking capabilities..." (!!). And if you are transmitting data over such networks, who is trusted with the keys to the encryption so that ballots cannot be changed at will?? Generally, we would prefer to see the vast majority of voters use hand-marked paper ballots that are processed in a central secure facility where there is no need to transmit data over networks.

We hope these comments will be helpful. It is our recommendation that the current draft of these principles NOT be approved at this time until they are more carefully drafted. We can be available to be involved in any drafting process that may be necessary to expedite the improvement of these principles so they can be eventually approved.

It would be very helpful to have the Requirements included with the Principles so they can be processed together.

Sincerely,



Raymond Lutz
Citizens' Oversight Projects
raylutz@citizenoversight.org
619-820-5321



May 29, 2019

VIA ELECTRONIC SUBMISSION

United States Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Re: Public Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

Disability Rights Florida appreciates the opportunity to comment on the draft Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines. Founded in 1977, Disability Rights Florida is the federally-mandated statewide protection and advocacy (P&A) system benefitting Floridians with disabilities through the provision of free and confidential legal and advocacy assistance. Our organization maintains authority under nine federal grants to pursue legal, administrative, and other appropriate remedies or approaches to safeguard and advance the rights of all individuals with disabilities in the state. The P&A network was established by the United States Congress to protect the rights of people with disabilities and their families through legal support, advocacy, referral, and education. Collectively, the P&A network is the largest provider of legally-based advocacy services to people with disabilities in the United States. Through the Protection and Advocacy for Voter Access (PAVA) program – created by the Help America Vote Act (HAVA) of 2002 – Disability Rights Florida maintains a federal mandate to “ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places.”

Our organization applauds the United States Election Assistance Commission (EAC) for attempting the complex task of balancing election security with federal elections accessibility requirements under law. However, Disability Rights Florida remains concerned that the only voting systems capable of meeting VVSG 2.0's requirements will be reliant on a marked paper ballot as the ballot of record, a concern that has been further confirmed by the technical standards proposed for the VVSG 2.0 that are currently being developed in public forums. It must be acknowledged that the promise of fully-accessible, paper-based voting systems is as old as the passage of HAVA itself more than fifteen years ago. In truth, the dream that paper ballots will be made more accessible, private, and implemented in a manner that these ballots are capable of being cast independently is not now, and may never be, a reality for voters with disabilities. Widespread implementation of market-ready, fully-accessible paper balloting election systems is simply not achievable within the foreseeable future.

Moreover, VVSG adheres to the misguided concept of “one accessible system per polling place.” The assumption that voting accessibility is limited to use of a ballot marking system at a traditional polling place neglects the rapidly-expanding opportunities to participate in the electoral process outside a visit to one’s neighborhood polling place. Increasingly, voters with disabilities and their non-disabled peers are

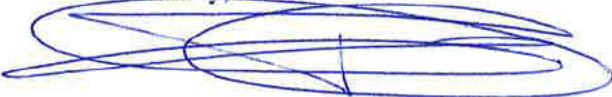
leveraging opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. Despite this, however, VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the reach and scope of these guidelines into these and other non-traditional voting systems.

Disability Rights Florida believes that the failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated electoral processes restrict any voter that benefits from use of an accessible voting system to a separate line – segregation of voters endeavoring to exercise a fundamental right in this fashion is inherently unequal and discriminatory, and should no longer be considered a standard, acceptable practice in the United States. In practice, segregated voting practices are already known to be riddled with problems for voters with disabilities. The assumption that a majority of voters will hand-mark their ballots means that there are a limited number of accessible voting machines present – consequently, poll workers are insufficiently prepared to operate such machines and are often unable to describe and activate accessibility features included in the equipment's design. When this is the case, in worst case scenarios elections personnel have been noted to discourage use of the equipment by voters or to leave the voting machine turned off, still in its case, or even hidden from view. For the few voters that are able to cast their ballots on the lone accessible system available, the secrecy of their ballots cannot be guaranteed as the balloting processes utilized inevitably vary in appearance from hand-marked ballots and may even be tallied and stored separately. Disappointingly, the accessibility ratios/quotas (arrived at in a similar manner to the number of accessible parking spaces required based on the size of a parking lot) and related requirements specifying that electronic voting technology produce a comparable ballot to those that are hand-marked remain outside the scope of VVSG 2.0.

While Disability Rights Florida believes that America's elections must be accurate and understands the intent to appear cybersecurity advocates, the VVSG is widely-used by voting technology manufacturers to guide the development of their products and by state-and-local election officials to inform their own purchase and implementation of voting equipment. It behooves EAC, in its efforts to comprehensively re-envision these guidelines, to expand the VVSG's reach to encompass all technology used to cast ballots within (or beyond) the traditional polling place. Further, the VVSG must ensure a private and independent ballot for all voters in a fully-integrated experience that respects the dignity of the voter, the secrecy of the ballot, and the integrity of the process.

Thank you again for the opportunity to submit these comments. If our organization can be of any further assistance in this or any other matters before the Commission, please do not hesitate to contact us directly.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tony DePalma".

Tony DePalma
Director of Public Policy
Disability Rights Florida



May 29, 2019

VIA ELECTRONIC SUBMISSION

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Public Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

Disability Rights North Carolina (DRNC) appreciates the opportunity to comment on the draft Voluntary Voting System Guidelines 2.0. Principles and Guidelines. DRNC is the non-profit Protection and Advocacy (P&A) agency for people with disabilities serving North Carolina. The P&As were established by the United States Congress to protect the rights of people with disabilities and their families through legal support, advocacy, referral, and education. P&As are in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Territories (American Samoa, Guam, Northern Mariana Islands, and the US Virgin Islands), and there is a P&A affiliated with the Native American Consortium which includes the Hopi, Navaho and San Juan Southern Paiute Nations in the Four Corners region of the Southwest. Collectively, the P&A Network is the largest provider of legally based advocacy services to people with disabilities in the United States. Through the Protection and Advocacy for Voter Access (PAVA) program, created by the Help America Vote Act, the P&As have a federal mandate to "ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places" and are the leading expert on access to the vote for people with disabilities in the United States.

DRNC applauds the US Election Assistance Commission (EAC) for attempting the complex task of balancing election security with federal elections accessibility requirements under law. Yet, DRNC remains concerned that the only voting systems capable of meeting VVSG 2.0's requirements will be reliant on a marked paper ballot as the ballot of record, a concern that has been further confirmed by the technical standards for the VVSG that are currently being developed in public forums. It must be acknowledged that the promise of fully accessible, paper-based voting systems is as old as the passage of HAVA itself. Yet, the dream that paper ballots will be made accessible, private, and able to be cast independently for people with disabilities is not now, and may never be, a reality. Widespread implementation of market-ready, fully accessible paper ballot voting systems is simply not achievable within the foreseeable future.

Further, VVSG 2.0 adheres to the misguided concept of “one accessible system per polling place.” The assumption that voting accessibility is limited to use of a ballot marking system at a traditional polling place neglects the rapidly expanding opportunities to participate in the electoral process outside a visit to one’s neighborhood polling place. Increasingly, voters with disabilities and their non-disabled peers are leveraging opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. Yet, VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the extent of the VVSG’s reach into non-traditional voting systems.

DRNC believes that the failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated electoral processes restrict any voter that benefits from use of the accessible voting system to a separate line, while more able-bodied voters hand mark their paper ballots. Segregated systems are a form of discrimination and inherently unequal and should no longer be considered a standard, acceptable practice in the United States. In practice, segregated voting practices are already known to be riddled with problems for voters with disabilities. The assumption that a majority of voters will hand mark their ballots means that there are a limited number of accessible voting machines present. Poll workers are insufficiently prepared to operate them. As a result, poll workers at their best are unable to describe and activate accessibility features included in the equipment’s design. At worst, elections personnel discourage use of the equipment by voters or leave the voting machine turned off, still in its case, and even hidden from view. For the few voters that are able to cast their ballots on the one accessible system available, the secrecy of their ballots cannot be guaranteed. The ballots inevitably vary in appearance from hand marked ballots and may even be tallied and stored separately. Disappointingly, the accessibility ratios/quotas (similar to calculating the number of accessible parking spaces required based on the size of a parking lot) and requirements that electronic voting technology produce a comparable ballot to those hand marked remain outside the scope of the VVSG.

While DRNC believes that our nation’s elections must be accurate and understands the intent to appease cybersecurity advocates, the VVSG is widely used by voting technology manufacturers to guide the development of their products and by state and local elections officials to inform purchase and implementation of voting equipment. It would be best for the EAC, in this process of a comprehensive re-envisioning of the guidelines, to expand the VVSG’s reach to encompass all technology used to cast ballots within or beyond the traditional polling place. Further, the VVSG must ensure a private and independent ballot for all voters in a fully integrated experience that respects the dignity of the voter and the secrecy of the ballot.

Thank you for the opportunity to comment on these important principles and guidelines. If you have any questions please contact Kenya Myers at 919-856-2195 or kenya.myers@disabilityrightsnc.org.

Sincerely,



Corye Dunn
Director of Public Policy



2222 W. Braker Lane
Austin, Texas 78758
MAIN OFFICE 512.454.4816
TOLL-FREE 800.315.3876
FAX 512.323.0902

May 29, 2019

VIA ELECTRONIC SUBMISSION

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Public Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

Disability Rights Texas (DRTx) appreciates the opportunity to comment on the draft Voluntary Voting System Guidelines 2.0. Principles and Guidelines. DRTx is Texas' designated Protection and Advocacy agency. We provide a wide range of services for people with disabilities, including training, education, and direct legal representation. We work to ensure that Texans with disabilities are not discriminated against on the basis of their disability. Further, through the Protection and Advocacy for Voter Access (PAVA) program, created by the Help America Vote Act, DRTx and all P&As have a federal mandate to "ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places" and are the leading expert on access to the vote for people with disabilities in the United States.

DRTx agrees with the comments of the National Disability Rights Network (NDRN), supporting the US Election Assistance Commission (EAC) attempt to balance election security with federal elections accessibility requirements under law. Yet, like NDRN, DRTx remains concerned that the only voting systems capable of meeting VVSG 2.0's requirements will be reliant on a marked paper ballot as the ballot of record, a concern that has been further confirmed by the technical standards for the VVSG that are currently being developed in public forums. It must be acknowledged that the promise of fully accessible, paper-based voting systems is as old as the passage of HAVA itself. Yet, the dream that paper ballots will be made accessible, private and able to be cast independently, for people with disabilities is not now, and may never be, a reality. Widespread implementation of market-ready, fully accessible paper ballot voting systems is simply not achievable within the foreseeable future.

Further, VVSG 2.0 adheres to the misguided concept of "one accessible system per polling place." The assumption that voting accessibility is limited to use of a ballot marking system at a traditional polling place neglects the rapidly expanding opportunities to participate in the electoral process outside a visit to one's neighborhood polling place. Increasingly, voters with disabilities and their non-disabled peers are leveraging opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. Yet, VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the extent of the VVSG's reach into non-traditional voting systems.

DRTx agrees with NDRN that the failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated electoral processes restrict any voter that benefits from use of the accessible voting system to a separate line, while more able-bodied voters hand mark their paper ballots. Segregated systems are a form of discrimination and inherently unequal and should no longer be considered a standard, acceptable practice in the United States. In practice, segregated voting practices are already known to be riddled with problems for voters with disabilities. The assumption that a majority of voters will hand mark their ballots means that there are a limited number of accessible voting machines present. Poll workers are insufficiently prepared to operate them. As a result, poll workers at their best are unable to describe and activate accessibility features included in the equipment's design. At worst, elections personnel discourage use of the equipment by voters or leave the voting machine turned off, still in its case, and even hidden from view. For the few voters that are able to cast their ballots on the one accessible system available, the secrecy of their ballots cannot be guaranteed. The ballots inevitably vary in appearance from hand marked ballots and may even be tallied and stored separately. Disappointingly, the accessibility ratios/quotas (similar to calculating the number of accessible parking spaces required based on the size of a parking lot) and requirements that electronic voting technology produce a comparable ballot to those hand marked remain outside the scope of the VVSG.

While DRTx believes that America's elections must be accurate and understands the intent to appease cybersecurity advocates, the VVSG is widely used by voting technology manufacturers to guide the development of their products and by state and local elections officials to inform purchase and implementation of voting equipment. It behooves the EAC, in this process of a comprehensive re-envisioning of the guidelines, to expand the VVSG's reach to encompass all technology used to cast ballots within or beyond the traditional polling place. Further, the VVSG must ensure a private and independent ballot for all voters in a fully integrated experience that respects the dignity of the voter and the secrecy of the ballot.

Thank you for the opportunity to comment on this important set of principles and guidelines. If you have any questions please contact Jeff Miller at 512-407-2762 or jmiller@drtx.org.

Sincerely,

Jeff Miller
Policy Specialist

AMY KLOBUCHAR
MINNESOTA

COMMITTEES:
AGRICULTURE, NUTRITION,
AND FORESTRY
COMMERCE, SCIENCE,
AND TRANSPORTATION
JOINT ECONOMIC COMMITTEE
JUDICIARY
RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510

May 29, 2019

The United States Election Assistance Commission
1335 East-West Highway
Suite 4300
Silver Spring, Maryland 20910

Re: Voluntary Voting System Guidelines 2.0 Public Comment

Thank you for the opportunity to comment on Version 2.0 of the Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG 2.0). These draft guidelines represent years of effort by elections officials, technical experts, and voting system makers to make vital updates to the VVSG to reflect known best practices and to counter cybersecurity threats in the modern era.

As you finalize these guidelines, I request that you consider the following recommendations to improve the VVSG 2.0 as well as the EAC's policies and processes for implementing the guidelines.

I. Vendors must support ongoing vulnerability research and disclosure

Principle 3 of the VVSG 2.0 states that voting systems and processes will be designed to provide transparency, and that the public can “understand and verify the operations of the voting system throughout the entirety of the election.” This is a critically important principle, and it is clear that public interest in verifying the integrity of our voting machines is strong. To meet this principle, members of the general public must feel safe and welcome to report security issues they discover in voting machines. Today, many security-conscious organizations that maintain critical systems accomplish this by operating vulnerability disclosure programs, where good-faith security research and reporting by the general public is encouraged and authorized. For example, since November 2016, the U.S. Department of Defense has maintained a policy authorizing public research and disclosure of security vulnerabilities on any of their public-facing websites.¹ Google², GSA³, Facebook⁴ and hundreds of other organizations across the public and private sectors operate similar vulnerability disclosure programs.

¹ <https://hackerone.com/deptofdefense>

² <https://www.google.com/about/appsecurity/>

³ <https://18f.gsa.gov/vulnerability-disclosure-policy/>

⁴ <https://www.facebook.com/whitehat>

Coordinated vulnerability disclosure programs that work with pre-vetted researchers are also a helpful aspect of a strong security program, particularly when granting those trusted researchers access to material not accessible to the public. However, these programs are not a substitute for the benefits of welcoming good-faith security research from the general public. In general, the overwhelming public interest and attention in our nation's election systems ensures that members of the general public will conduct security research on our voting machines and other election systems, regardless of what vendors do to encourage or discourage this practice. Well-designed vulnerability disclosure programs create guidelines and norms that can channel these research efforts constructively, and can incentivize both system owners and security researchers to address security vulnerabilities rapidly and privately.

Accordingly, I request that you consider the following recommendations in support of vulnerability disclosure:

- VVSG 2.0 Principle 3 should add a guideline that says that good-faith security research from the public is welcome, and ensure that voting system manufacturers have a clearly published, secure, and monitored channel for reporting issues.
- Going forward, the VVSG 2.0 certification process should condition certification on the vendor maintaining a vulnerability disclosure program that follows the best practices of other high-performing vulnerability programs, is applicable to the general public, and supports the anonymous submission of vulnerability reports. Such a program should include clear policy language authorizing good-faith security research that reduces the real or perceived risk of legal retaliation against researchers through the Computer Fraud and Abuse Act (CFAA) and other similar laws. Many similar policies ask researchers to agree to report vulnerabilities initially directly to the vendor and avoid public disclosure, until the vendor has had a reasonable time frame to investigate and respond to the report. In the case of voting machines, these policies might need to take into consideration the constraints of election timeframes, as well as the realities of deployed hardware and the certification process.
- This condition should be ongoing after certification, and the EAC should develop a process to revoke certification from systems made by vendors who are inhibiting good-faith security research into those systems.
- The EAC's processes for re-certification and approving security patches should be updated to explicitly accommodate the expected workflow for vulnerabilities reported by external security researchers, including affordances for involving the reporting researcher in the certification process, if appropriate and as needed to accelerate fixing the security issue. Overall, these process updates should reflect the public's expectations that fixes for significant and exploitable security vulnerabilities can be deployed in a reasonable but sufficiently rapid timeframe to ensure the integrity of affected upcoming elections.

II. Support flexible approaches to least privilege and reducing attack surface

Guideline 11.4 states that “Default access control policies enforce the principles of least privilege and separation of duties.” However, “access control policies” may leave the impression that least privilege is expected to be performed principally in software. For example, section 7 of VVSG 1.1 Voting System Performance Guidelines, Security Requirements, generally emphasizes software-based protections, such as process privileges, or file permissions, or validating firmware signatures. The principle of least privilege can also be expressed by isolating physical components, and designed to limit the damage of the compromise of any individual component’s software.

For example, if a voting system is designed only to make specific network connections to known hosts (e.g. DNS names), or using known protocol methods (e.g. HTTP GET), the software responsible for generating these network requests could be made to issue these network requests through a separate component whose sole function is to proxy network connections while applying a whitelist of expected destinations and protocols. This would mitigate the risk of compromise of a component which contains a full network software stack, and potentially would require an attacker to compromise both components in order to successfully connect the main voting system software to a network device controlled by the attacker. In general, the VVSG and EAC should encourage vendors to pursue all approaches to implementing the principle of least privilege than those offered within general-purpose operating systems.

Guideline 14.2 emphasizes the importance of reducing attack surface in software and hardware. However, guideline 15.3 states that a voting system “employs mechanisms to protect against malware”, which could be commonly understood to refer to antivirus software. These guidelines are in tension with each other. Many antivirus programs are implemented by placing the antivirus program itself in a highly privileged position within the host, which can create significant attack surface. The VVSG should more clearly indicate that alternate approaches at mitigating the effects of malware, including system designs that limit the potential impact of malware through the principle of least privilege, are encouraged and acceptable.

Accordingly, I request that you consider the following recommendations in support of reducing attack surface:

- Guideline 11.4 should be more explicit about pointing to hardware-based approaches to least privilege. For example, 11.4 could say “Default access control policies and hardware design enforce the principles of least privilege and separation of duties.”
- Guideline 15.3 should be less prescriptive in its language about malware resistance. For example, 15.3 could say “The voting system is designed to protect against malware.”
- EAC should encourage vendors in its certification documents and processes to consider approaches that rely on componentization of hardware and other approaches that mitigate the impacts of malware and increase attack cost.

III. Promote agility and security by separating policy from technical requirements

Best practices in technology, usability, accessibility, and cybersecurity change rapidly. It is imperative that voting systems in the United States are incentivized to keep pace with developments in these areas and follow known best practices, rather than lag behind other sectors. For the EAC’s certification program to remain relevant and authoritative over time, and for its requirements to be seen as a floor and not a ceiling, it is critical that the EAC’s standards for certification are able to continuously evolve.

As the VVSG 2.0 nears finalization, the EAC should follow the recommendations of the resolutions passed by its Board of Advisors⁵ and Standards Board⁶, and ensure that expert staff within the Commission can work with other technical experts to update the VVSG technical guidelines as necessary to keep up with developments in technology.

Accordingly, I request that you consider the following recommendations regarding EAC technical requirements:

- Before finalizing the VVSG, the EAC should adopt a policy that generally allows the updating of requirements and test assertions without an EAC commissioner vote, so that the EAC’s certification program can continue to rapidly evolve to meet the challenges of tomorrow. This policy itself would be subject to a vote by EAC commissioners, and could always be updated by the EAC commissioners in the future if unforeseen problems emerge from the implementation of this policy.

IV. Proactive information sharing with the public

Guideline 3.3 states that the public can “understand and verify the operations of the voting system throughout the entirety of the election.” To support this, the EAC should institute a policy of proactive disclosure of documents submitted by vendors, and publish these documents on their website by default. The current EAC Voting System Testing and Certification Program Manual, version 2.0, states in section 10 that EAC will release materials to the public through the Freedom of Information Act (FOIA). This policy establishes limited transparency, as it requires public research and action in order for any documents to be released. The public should not have to file a legal request in order to get non-sensitive information about the voting machines used in our elections.

The benefits of transparency go beyond documentation, and may extend to source code. For example, earlier this year security researchers identified a serious security flaw⁷ in the e-voting system developed by Scytl for the Swiss Post⁸. The researchers were only able to discover this flaw by analyzing the source code for the voting system.

⁵ <https://www.eac.gov/documents/2018/04/27/resolution-2018-01-advance-vvsg-passed-21-0-advisors-resolution-page/>

⁶ <https://www.eac.gov/documents/2018/04/27/standards-board-vvsg-resolution-2018-01-advance-vvsg-standards-resolution-page/>

⁷ <https://people.eng.unimelb.edu.au/vjteague/SwissVote>

⁸ <https://www.zdnet.com/article/vulnerability-in-swiss-e-voting-system-could-have-led-to-vote-alterations/>

Guideline 2.4 states that the “voting system structure is modular, scalable, and robust”. If a voting system is designed to be modular, it is reasonable to expect that the source code required for operations that ensure basic voting integrity (such as tabulation logic, and the implementation of protocols and libraries that ensure secure network communications) can be cleanly separated from the source code required to perform vendor-proprietary or brand-differentiating operations (such as design layout).

Currently, source code supplied to the EAC by vendors during certification is generally not made publicly available. However, the EAC is certifying voting systems in order for them to be used to securely conduct elections for the public benefit. Since VVSG 2.0 would require that voting systems be modular, the EAC should consider requiring that vendors identify the modules in their code that are used to ensure basic voting integrity and then make them available for public review. The availability of these portions of source code, in standard machine-readable form, would dramatically improve the ability of security experts to provide beneficial review. The EAC’s process would not need to release other source code modules identified by vendors as proprietary.

Accordingly, I request that you consider the following recommendations in support of information sharing:

- The language of VVSG Principle 3 should be changed to more clearly require proactive disclosure of vendor-supplied documentation. For example, 3.1 could end with, “can be understood and read online at any time.”
- The EAC should adjust its policy to require vendors to identify – at submission-time – any potential trade secrets or other non-releasable information. The EAC should use this information to adjudicate releasable information and publish it online as soon as practical, but no later than at the time of certification.
- The EAC should require vendors to identify the modules of their source code that are non-proprietary and critical to voting integrity, such as those that perform basic tabulation and security operations, and make these modules available for public review.

V. **Vendors and labs should be directly connected to practicing technical and design experts**

Principle 2, High Quality Implementation, contains a number of excellent guidelines that support the development and design of high quality software. However, best practices in software development and user-centered design have changed substantially in recent years, and will continue to rapidly evolve. It would be valuable for the EAC to implement the VVSG so that current software practitioners can be part of an independent feedback and review process for voting systems, especially before they are submitted for certification. The intended outcome should be that election system makers are encouraged to seek candid and private feedback from independent practitioners on the specific designs of their machines and systems, as early in the development process as possible.

Accordingly, I request that you consider the following recommendation:

- EAC should identify a practical method to implement VVSG Principle 2 by connecting the designers of voting systems intended for submission to EAC for certification to active practitioners in modular software, user-centered design, and information security.

I'd like to thank the Commission for its work on VVSG 2.0. I look forward to working with you as the process moves forward.

Sincerely,



Amy Klobuchar
United States Senator

PUBLIC SUBMISSION

As of: June 14, 2019
Received: March 05, 2019
Status: Pending_Post
Tracking No. 1k3-981z-v41v
Comments Due: May 29, 2019
Submission Type: Web

Docket: EAC_FRDOC_0001

Recently Posted EAC Rules and Notices.

Comment On: EAC_FRDOC_0001-0077

Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines

Document: EAC_FRDOC_0001-DRAFT-0005

Comment from Cheryl Das

Submitter Information

Name: Cheryl Das

Address:

1421 Newton Ave.
Batavia, IL, 60510

General Comment

I am very much in favor of the Voluntary Voting System Guidelines 2.0 (VVSG 2.9) which provide a thorough blueprint for testing the reliability, accuracy and security of election equipment. It also includes updated requirements for voting system accessibility and security, including a call for paper ballots to facilitate election audits. I am extremely worried about possible hacking and the changing of ballots. I hope every state adopts these guidelines to reduce the possibility of election fraud via hacking and the wrong reporting of votes.

Comment on The Proposed Voluntary Voting Systems Guidelines 2.0

David Wilson

Master of Public Administration Student

University of North Florida

Executive Summary

In the U.S. eligible voters have the right to cast a ballot in free and fair elections. Over time, elections have become less prone to misconduct. However, they are still susceptible to certain types of fraud, especially insider fraud. Current voting systems are vulnerable to deliberate manipulation and may produce errors, especially as they age. Voting systems that do not work correctly reduce the public confidence in elections (Hasen, 2012; Pérez, 2017; Thompson, 2008). This makes the updated Voluntary Voting System Guidelines 2.0 (VVSGs) extremely important in keeping voting system integrity and defending against abuses that threaten election security and discourage fraud without overly burdening eligible voters. The guidelines also supply guidance to local election administration officials (EAOs), many of which do not have specialized skills in evaluating voting systems (Hasen, 2012; Thompson, 2008). This is especially important because most states have voting systems that are either out of production or at least 10 years old. Many of the states are planning to replace the obsolete voting systems before the 2020 election.

This comment supports the proposed Voluntary Voting System Guidelines 2.0 and it recommends several improvements to these guidelines. The improvements include the following additions and changes to the guidelines:

- Provide concrete examples of each principle and guideline to help EAOs evaluate voting systems.
- Provide a rubric either as part of the VVSGs, or as a supplementary document to enable EAOs to compare certified voting systems.
- Rank the importance of each principle to enable EAOs to make more informed decisions when choosing a certified voting system.

- Create a principle to address the cost of voting machines. This is especially important because many local election jurisdictions report that even with assistance from the EAC they will still not have sufficient funding to purchase enough new voting systems.
- Create a principle to address the maintenance and operation of voting systems.
- Create a principle to address the lifecycle issues of voting systems.
- Incorporate Norden's (2006) recommendations for improving voting system security into the VVSGs.

Merits of the Voluntary Voting System Guidelines

The VVSGs are important for several reasons. They give local election boards a consistent and accurate voting experience and a framework for operation, security, and maintenance of voting systems. Systems that meet the guidelines and are certified by the Election Assistance Commission (EAC) will provide Chief Election Officials (CEOs) the ability to respond to candidate claims of equipment malfunction and manipulation and increase voters' confidence that their vote will be counted correctly. VVSGs also help private businesses in the industry because they combine smaller, local markets into larger more workable markets. Many of the nation's voting systems are old and need to be replaced (Hale & Brown, 2013; Norden & Cordova, 2019).

Most of the states (45) are using voting systems that are out of production. Additionally, 40 states are using voting systems that are at least 10 years old. As systems get older, they start to need more repairs and become less reliable; and it is extremely difficult to get spare parts for the systems that are no longer manufactured. The aging systems are not secure because the software they use is no longer being updated (Breitenbach, 2016; J.E.F, 2019; Norden &

Cordova, 2019). Also, older systems may be less accurate and produce more overcounts and undercounts (Thompson, 2008). There have been reported errors of Direct Recording Electronic (DRE) machines switching votes or not allowing voters to select a candidate (Thompson, 2008). Some of these systems do not produce paper copies of ballots that can be verified by voters during the voting process and used in manual recounts. Additionally, the source code used by these systems are proprietary, not open, and cannot be reviewed by election administrators. In some cases the system manufactures provide the system source code to the CEOs, but many CEOs do not have staff qualified to review the code (Thompson, 2008). Many states would like to replace these machines before the 2020 election. VVSGs provide a level of federal guidance to the decentralized election system. Having new, updated VVSGs would assist states in making decisions on which voting systems to purchase. This is important because some states do not have the resources to develop voting systems guidelines independently.

Recommendations

This comment supports the new VVSGs. Nevertheless, it provides recommendations for their improvement. The proposed guidelines are a “high-level system design.” They are intended to be used by election officials in conjunction with separate documents that detail how voting systems can meet the guidelines and test assertions on how the voting systems will be tested for certification (Election Assistance Commission, 2019). Even though these guidelines are not intended for use by election officials without other documents, they would still benefit from concrete examples for each of the listed recommendations. Election administration officials typically do not have specialized expertise in voting systems, especially newer digital systems (Hale & Brown, 2013; Hasen, 2012; Thompson, 2008). They may have problems incorporating the high-level recommendations to the decision-making process when purchasing new voting

systems. For example, Principle 4.1 “Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.” Could include an example like: “The system will import and export data using a format like comma separated values (CSV), or the Microsoft Excel file format.”

Another issue with the proposed guides is that they are a list of 15 principles that voting systems should adhere to without ranking the relative importance of each principle as compared to other principles. Also, it does not give EAOs the information to compare voting systems when deciding which system to purchase. Say, for example an EAO is deciding between purchasing one of two different voting systems, system A and system B for the voting district. Both systems are certified; but A outperforms B in Principle 1: High Quality Design and B outperforms A in Principle 2: High Quality Implementation. It is not clear, based on the principles, which system the EAO should select. In this situation, administrators may select a voting system arbitrarily, or based on other, less crucial factors. While the importance of all the principles in the guidelines is clear, guidelines directly affecting voter turnout are of greatest importance, followed by those that provide the greatest voting experience, then those that affect accuracy and secrecy, and finally those that affect the security, operation, and maintenance of the systems. The VVSGs should include, either in the guidelines themselves, or as supplementary material, rubrics for rating systems on each of the principles and guidelines it contains. This would enable election administration officials to actually compare different certified voting systems and make informed decisions. Additionally, it would allow certified voting system testers the ability to give each system an overall rating, a rating on each principle, and a rating on each guideline. Not only would EAOs be better informed but voting system manufacturers would have standardized feedback on how their systems compare to other systems and how they can be improved.

One of the issues facing local election authorities is the cost of voting systems. Even with assistance from the EAC, many voting districts struggle with being underfunded and unable to replace old machines. Not only does the VVSGs not address this issue, the guidelines do not acknowledge it at all. The guidelines should include principles of economy and efficiency. The reality of the national election environment is that system cost is a major issue (Hasen, 2012; Thompson, 2008). Furthermore, economy and efficiency are pillar principles of public administration that should be embedded in every governmental process at every level: federal, state, and local (Denhardt & Denhardt, 2000). It is possible to include principles that would reduce the cost of the initial purchase of voting systems and their maintenance. For example, a principle could be added that called for the use of free open source software and hardware. This would reduce the initial cost of the voting systems and it would reduce the cost of system maintenance. The principle could also call for modular hardware that could easily be replaced by non-specialized staff at any time. This would reducing the downtime of a broken voting system during elections. The VVSGs should also include principles that address voting systems life-cycles. A current issue faced by many election administrators is that they have old machines that are not performing optimally, this is especially true of the DRE machines (Thompson, 2008). The VVSGs should also include guidelines to recommend a minimum operating lifespan, a minimum number of processed ballots, and a minimum warranty term for voting systems.

Voting system security is addressed by the VVSGs. However those principles and guidelines could be improved by adopting the recommendations of Lawrence Norden and the Brennan Center Task Force on Voting System Security (2006). They include conducting automatic routine audits to compare paper records with electronic counts using statistical sampling, performing parallel testing on voting systems on election day, banning wireless

components on voting machines, using transparent and random selection processes for all auditing procedures, using decentralized programming and system administration, and instituting clear, effective procedures to address evidence of fraud or error.

Conclusion

This comment supports the Voluntary Voting System Guidelines 2.0 proposed by the Election Assistance Commission and makes recommendations for their improvement. The VVSGs are necessary to assist election administration officials in their decision-making processes for selecting new voting systems. The recommendations for improvement include: providing concrete examples for each guideline and principle, creating a rubric to allow EAOs to better evaluate certified voting systems, include principles to address the cost of voting systems, their maintenance and operation, and the lifecycle of voting systems. The principles should also be updated to incorporate the recommendations identified by Norden. Finally, the principles should be organized in a way to inform people to the relative importance of each principle when compared to the other principles with a focus on making the voting process as easy and accessible as possible, followed by accuracy, security, maintenance and operation, economy, and lifecycle.

Works Cited

- Breitenbach, S. (2016, March 2). Aging Voting Machines Cost Local, State Governments. Retrieved April 6, 2019, from Pew Charitable Trusts website: <http://pew.org/1oNbZl1>
- Denhardt, R. B., & Denhardt, J. V. (2000). The New Public Service: Serving Rather than Steering. *Public Administration Review*, 60(6), 549–559. <https://doi.org/10.1111/0033-3352.00117>

Election Assistance Commission. (2019, February 28). *Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines*. Retrieved from

https://www.regulations.gov/document?D=EAC_FRDOC_0001-0077

Hale, K., & Brown, M. (2013). Adopting, Adapting, and Opting Out: State Response to Federal Voting System Guidelines. *Publius: The Journal of Federalism*, 43(3), 428–451.

<https://doi.org/10.1093/publius/pjt016>

Hasen, R. (2012). *The Voting Wars: From Florida 2000 to the next Election Meltdown*. Grand Rapids, MI: Yale University Press.

J.E.F. (2019, March 6). Voting machines across America are old and inadequate. *The Economist*. Retrieved from <https://www.economist.com/democracy-in-america/2019/03/06/voting-machines-across-america-are-old-and-inadequate>

Norden, L. (2006). *The Machinery of Democracy: Protecting Elections in an Electronic World* (p. 162). BRENNAN CENTER TASK FORCE ON VOTING SYSTEM SECURITY.

Norden, L., & Cordova, A. (2019, March 5). Voting Machines at Risk: Where We Stand Today | Brennan Center for Justice. Retrieved April 6, 2019, from <http://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today>

Pérez, M. (2017). *Election integrity: a pro-voter agenda* (p. 48).

Thompson, C. (2008, January 6). Voting Machines - Elections - Ballots - Politics. *The New York Times*. Retrieved from <https://www.nytimes.com/2008/01/06/magazine/06Vote-t.html>

May 23, 2019

Commissioner Christy McCormick
Chairwoman
United States Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, Maryland 20910

Submitted electronically via www.regulations.gov

Re: Comments from the Bipartisan Policy Center on EAC's Proposed "Voluntary Voting System Guidelines 2.0 Principles and Guidelines" (Docket ID No. EAC_FRDOC_0001)

Dear Chairwoman McCormick:

The Bipartisan Policy Center is a nonprofit organization that combines the best ideas from both parties to promote health, security, and opportunity for all Americans. BPC drives principled and politically viable policy solutions through the power of rigorous analysis, painstaking negotiation, and aggressive advocacy. Our policy solutions are the product of informed deliberations by current and former elected and appointed officials, business and labor leaders, and academics and advocates who represent views from across the political spectrum.

BPC is pleased to submit comments on the U.S. Election Assistance Commission's proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines. BPC's Elections Project builds on the success of our efforts to enhance the voting experience by implementing the recommendations of the Presidential Commission on Election Administration. The Elections Project has convened three task forces in 2019 to analyze voting in America, develop bipartisan recommendations that improve the voting experience, and engage in the 2020 election conversation with respect to registering to vote, casting a ballot, and counting the vote. The Elections Project maintains relationships with local and state election administrators and policymakers and administers the largest data collection of line lengths at individual polling places throughout the country.

The proposed standards are the result of years of work by experts, administrators, and policymakers throughout the government, nonprofit, and advocacy sectors. All should be commended for their dedication to America's voters.

Voters expect and deserve voting systems 1) on which they can make and change selections in an accessible, private, and independent manner with safeguards against inadvertent invalidation of their results, and 2) that produce an auditable record.

The proposed structure of the new VVSG as principles and guidelines for EAC commissioner adoption—along with separate technical requirements and test lab assertions that do not require commissioner adoption—will result in the development of voting technology that meets

federal standards and improves the voting experience without the additional risk of partisan or quorum concerns.

The EAC seeks feedback regarding all sections of the Voluntary Voting System Guidelines 2.0 Principles and Guidelines including the proposed structure of VVSG 2.0. BPC supports all 15 high-level principles as essential components of a voting system that works for the voter and increases confidence in end results. We have no comment on the specific principles and guidelines proposed.

Our comment, therefore, focuses on the new structure for VVSG 2.0. We support this new structure for three reasons:

1. The local and state election administrator community strongly endorses a structure for VVSG 2.0 that separates out the principles and guidelines from the technical requirements and voting system testing lab assertions. In fact, the National Association of State Election Directors (NASED) VVSG committee should be credited with proposing the new structure for the Voluntary Voting System Guidelines, as that group started focus on these changes more than five years ago. The EAC's own Board of Advisors and Standards Board endorsed the structure. Those two boards include nearly 150 local, state, and national experts representing every state in the country and numerous interests identified by Congress during the drafting of the Help America Vote Act of 2002. The Technical Guidelines Development Committee has also endorsed this new structure. These boards are meant to provide EAC commissioners a real-time assessment of the election official and advocacy community as EAC works to further its mission to help election officials improve the administration of elections and Americans participate in the voting process. They are intent on creating consistent, implementable guidelines for which technical requirements and testing lab assertions can be updated in short order by voting system technical experts as technology evolves.
2. While there is a full complement of commissioners now serving on at the EAC, that is not always the case, and BPC cannot endorse a structure of VVSG 2.0 that is inflexible should quorum issues reemerge at some point in the future. We expect the principles and guidelines to require review every few years while the technical requirements and voting system testing lab assertions may need more regular updating as new technology is invented and enters the market.

Based on a [BPC analysis from December 2018](#), the EAC has had all four commissioner slots filled simultaneously for less than a third of its time in existence. Between the beginning of 2012 and the end of 2018, there was an operational quorum of three commissioners less than half the time. The EAC's lapse in maintaining current, state-of-the-art guidelines can be traced directly to its quorum issues. This fact undermines Americans' confidence in the voting systems when they hear the systems in use today are built on guidelines that were mostly written more than a decade ago.

3. The structure of the EAC as strictly bipartisan was smart and the vast majority of EAC actions have been adopted unanimously. Election policy should be endorsed by Republicans and Democrats together through the political appointees on the EAC.

However, one needs only to look at the U.S. Federal Election Commission to see that partisanship can hamstring a bipartisan agency. While the principles and guidelines of the voluntary voting system guidelines are a policy level consideration appropriate for the commissioners' attention, the technical requirements and voting system testing lab assertions are procedural documents that do not implicate policy concerns and should not be subject to future partisan disagreement.

Voting system experts at the National Institute of Standards and Technology (NIST) and on the EAC staff need flexibility in maintaining and evolving the technical requirements and voting system testing lab assertions to ensure Americans regain and keep confidence that the voting technology is free from partisanship.

A new structure of VVSG 2.0 that codifies sub-commissioner level changes to the technical requirements and voting system test lab assertions could also allow for a policy change by which the full commission becomes the appeals panel to any NIST and EAC staff decisions to update the technical requirements and voting system test lab assertions. However, any such policy should be structured in a way that allows the process to move forward until a commission vote is taken that overturns a NIST and EAC staff decision. This structure maintains a strong and important role for the commissioners in overseeing the testing and certification of voting systems in situations where policy-level concerns may arise while avoiding the aforementioned quorum issues that have halted the process in the past.

In conclusion, BPC strongly believes that the new structure of VVSG 2.0 is better for election officials, vendors, and, most importantly, American voters. BPC encourages the EAC to consider these comments as it endeavors to create voluntary voting system guidelines that reflect modern technological advancement and that work in today's political environment.

Sincerely,

Matthew Weil
Director, Elections Project
Bipartisan Policy Center



Republican National Lawyers Association

P.O. Box 18965 • Washington, D.C. 20036 • Phone: (202) 802-0437 • <http://www.rnla.org>

TO: United States Election Assistance Commission
FROM: Republican National Lawyers Association
DATE: May 29, 2019

Thank you for the opportunity to comment on the Voluntary Voting Systems Guidelines (VVSG) 2.0 Principles and Guidelines.

The Republican National Lawyers Association (RNLA) is the home of Republican lawyers in the Republican Party. The missions of the RNLA are advancing professionalism; advancing open, fair, and honest elections; advancing career opportunities; and advancing Republican ideals. Since 1985, RNLA has worked to ensure elections are open, fair, and honest so that every eligible voter's vote is counted and ineligible votes are not counted.

The United States has the finest election system in the world and enjoys a proud position as the leading, longest lasting representative democracy in the world. Yet, there is always work to be done to improve the election system, and updating the VVSG is an important step for the Election Assistance Commission (EAC) to take to bring the certification standards for many voting systems used in America up to date with modern technological standards. The EAC should be commended for undertaking to update the VVSG quickly after a quorum of commissioners was re-established and for providing ample opportunity for public input through written comments and public hearings.

While states and localities have the primary responsibility to administer elections under our federalist system established by the Constitution, the EAC has an important role on the federal level to assist the states in administering their elections by sharing information, identifying best practices, and establishing voluntary standards. The bipartisan structure of the EAC, requiring the votes of at least three commissioners representing two of the major political parties for official agency action, is vital to its legitimacy as a federal resource to the states.

While updating the VVSG is an important goal, it is vital that the EAC not abandon these two foundational principles in the process: bipartisan control of election standards and the primary role of the states in election administration. The EAC's respect for these two principles are what gives the agency its legitimacy and what have made it a successful, trusted federal partner for election officials around the country.

Proposed VVSG 2.0 Principles and Guidelines

The proposed high-level Principles and Guidelines document¹ provides worthy goals for guidelines on voting system, but the terms used throughout the document need to be defined. The terms as currently written are vague and ambiguous and subject to differing interpretations. This may cause confusion for election officials and vendors who are seeking to create systems that meet the requirements of VVSG 2.0.

¹ U.S. Election Assistance Commission, Technical Guidelines Development Committee, Voluntary Voting System Guidelines 2.0, Principles and Guidelines [Draft], Sept. 12, 2017, available at https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.

It is important for manufacturers of voting systems to have clear Principles and Guidelines and specific corresponding Requirements together in order to be able to design systems that comply with the VVSG and obtain certification. There must be no ambiguity so manufacturers can rely on the Requirements and invest in creating or updating systems that will be compliant. Manufacturers will be unwilling to make this investment if the Principles and Guidelines or Requirements are vague, with undefined terms, as they would risk investing in a new system without the system being certified under the VVSG.

Reliability is essential to the VVSG process, including assurance for voting system vendors that there will not be sudden changes or modifications that may be costly to the design and manufacturing process and ultimately impact the purchase price. Uncertainty in the VVSG standards will be reflected in a higher price for the voting systems offered to states and localities, stressing the limited resources of election officials as they seek to invest in modern technology and update their systems.

Process for VVSG 2.0 Approval and Implementation

The Help America Vote Act of 2002 (HAVA) provides a process for the implementation of the VVSG that must be followed. VVSG 2.0 must consist of both the proposed high-level Principles and Guidelines together with the corresponding Requirements that, importantly, will also be subject to public review and comment. The Requirements, as part of the final VVSG 2.0, must have commissioner oversight and be voted on by the Commission before implementation to meet the requirements of HAVA.² The bifurcated method of consideration and adoption for the VVSG 2.0, dividing the VVSG into Principles and Guidelines and separate Requirements, does not remove the requirement for bipartisan approval by the EAC commissioners. Indeed, this approval is vital to the legitimacy of the VVSG.

The proposed Principles and Guidelines and the Requirements, once developed, cannot be considered separately or as different policies. The Requirements must be attached to the high-level Principles and Guidelines for clarity, context, and understanding and the two documents must only be considered and voted on together. Together, they are what HAVA contemplates as the Voluntary Voting Systems Guidelines, and only when paired can they provide clarity for election officials and voting system vendors on what the requirements for certification are under VVSG 2.0.

In conformity with HAVA, the Standards Board and Board of Advisors must be given an opportunity to provide input on the Principles and Guidelines together with their specific corresponding Requirements. These boards must also be given an opportunity to provide input on any subsequent modifications or updates to the Principles and Guidelines along with their specific corresponding Requirements.³ Similarly, there must be an opportunity for public comment on the Principles and Guidelines together with their specific corresponding Requirements and also on any subsequent modifications or updates to the Principles and Guidelines together with their specific corresponding Requirements.⁴

Due to the EAC lacking a quorum of commissioners for nearly a year, there have been proposals for EAC staff to approve changes or updates to the VVSG, instead of the commissioners. There are several problems with such a proposal. First, HAVA requires a vote of the commissioners prior to the final adoption of the VVSG or a modification of the VVSG.⁵ Thus, a change to the VVSG approval process would require Congress to amend HAVA; this is not a procedural change that can be made on the agency level.

² Help America Vote Act of 2002, 52 U.S.C. § 20962(d) (2019) (A voluntary voting system guideline . . . shall not be considered to be finally adopted by the Commission unless the Commission votes to approve the final adoption of the guideline (or modification), taking into consideration”).

³ *Id.* § 20962(b).

⁴ *Id.* § 20962(a).

⁵ *Id.* § 20962(d).

Second, removing oversight and approval of the VVSG from the commissioners—who are suggested by congressional leaders, nominated by the President, confirmed by the Senate, and must act in a bipartisan manner—and placing it with unaccountable staff, however excellent the EAC staff may be, threatens the legitimacy of the VVSG itself. Bipartisan approval of the standards governing our elections is vital to ensuring that our election systems are open, fair, and honest both in appearance and actuality. Removing bipartisan oversight would decrease public confidence in the VVSG and reduce buy-in by the community of election officials.

If there is a lack of quorum on the EAC, changes or modifications to the VVSG, including implementation of new Requirements, must wait until a quorum of commissioners is re-established. The only exception could be a change or update made due to an update or change to an external standard referred to in the VVSG, as long as an implementation of this updated external standard in the VVSG does not materially impact the other current Requirements. Whether there is a quorum on the EAC is a political question for Congress to decide and is not the responsibility of the commissioners or EAC staff.

The EAC should not and cannot attempt to bypass the authority of Congress. The Requirements, as they correspond to the high-level Principles and Guidelines, are policy governed by the procedures in HAVA and must be kept in and under the domain of the commissioners as political appointees who act in a bipartisan manner, as outlined in HAVA.

By updating the VVSG in an open, transparent, bipartisan process, the EAC has an opportunity to improve the public's confidence in the reliability of the voting systems, the voting process, and the outcomes of elections across America. The RNLA thanks the EAC and its commissioners for undertaking this important work and for assisting state and local election officials as they administer one of our most important American institutions.

If you have any questions about this comment, please contact Michael Thielen, RNLA Executive Director, at thielen@republicanlawyer.net or 202-802-0437.



Verified Voting.org

Public Comments on VVSG 2.0 Principles and Guidelines

Submitted May 29, 2019

Verified Voting is pleased to see the VVSG 2.0 principles and guidelines finally moving forward. We are enthusiastic about the VVSG 2.0 structure and, with some reservations, about the content of the principles and guidelines. Full implementation of the VVSG 2.0 will, in time, help bring about voting systems that set new standards for universal usability, security, and verifiability. All these properties – backed by sound procedures – are essential to enable officials to run resilient elections, and to reassure voters that their votes have been cast as intended and counted as cast.

We urge the EAC to allow the technical requirements and test assertions to be approved and revised without a vote of the commissioners. We agree with the TGDC, the NASED executive council, and others that for several reasons, these documents are best managed by technical staff, adhering to a well-defined process with broad consultation and opportunity for public comment.

Verification and the VVSG

Verified Voting especially welcomes Principle 9, which stipulates that a voting system “is auditable and enables evidence-based elections,” and the associated guidelines. No matter how otherwise usable and reliable a voting system may be, it is unacceptably dangerous if it cannot provide trustworthy, software-independent evidence that people’s votes have been accurately recorded and counted.

A voting system alone can “enable” evidence-based elections but cannot provide them. As Philip Stark and David Wagner wrote in their seminal paper, the basic equation is that “evidence = auditability + auditing.” A voting system with a voter-verifiable audit trail, such as a voter-marked paper ballot, provides auditability. Compliance audits to ensure that the audit trail is substantially complete and accurate, and risk-limiting tabulation audits of the audit trail, provide actual evidence that outcomes are correct.

These considerations point to two ongoing challenges for the EAC and everyone else who works with the VVSG. One challenge is to communicate

that, in practice, voting system security largely depends on election procedures and especially on post-election audit procedures. Compliance and risk-limiting tabulation audits happen after elections but cannot be afterthoughts: evidence-based elections depend on them.

The other challenge is to frame requirements and test assertions that help to move auditability from an abstract possibility to a standard of excellence. One lesson of the Help America Vote Act era has been that a voting system may be formally “accessible” without being very usable by the voters who need it most. Similarly, a voting system may be “verifiable in name only” if its audit trail is difficult for voters to verify and/or for authorities to audit.

Voting systems should be rigorously tested to see if voters consistently and effectively verify their paper ballots or other auditable records in a variety of election conditions. (See the discussion of “ballots” below.) The systems also should be assessed for ease of auditability. The most auditable paper-based systems not only provide paper records that are easy for audit officials (as well as voters) to handle and to verify, but allow each paper record to be matched with the corresponding digital cast vote record(s) without compromising ballot anonymity.

Ballots and cast vote records: definitions and implications for auditability

In common parlance, ballots are paper records of voters’ votes, and cast vote records are digital representations of the votes on the ballots. To accommodate alternative models, the glossary that accompanies the VVSG defines “ballot” as a “presentation of the contest options for a particular voter,” and “cast vote record” as an “archival tabulatable record of all votes produced by a single voter from a given ballot.” In this framework, a ballot could be physical or digital, as could a cast vote record.

These expansive definitions seem to account for several confusing points in the principles and guidelines, such as 6.2’s reference to casting a cast vote record. They also complicate discussions of auditability. In a system based on paper ballots, the paper ballots can be verified and cast by voters and then audited. In systems that do not use paper ballots – even if they produce an auditable paper record – verifying and casting the ballot does not assure that the voter has verified the auditable record. If we could make just one change to the principles and guidelines, it would be to clarify in principle 7 and the associated guidelines that voters must be able to readily verify the records that will be retained and used to check whether the election outcome is correct (guideline 9.2).

Moreover, we believe that for the foreseeable future, only voter-verifiable paper records should be used for this purpose. Given the inherent vulnerabilities of today’s internet, no voting system that relies on digital records alone can provide truly secure and verifiable elections.

Specific comments

Principles 1 and 2: High Quality Design and Implementation

These principles are well framed, and we generally support the associated guidelines, particularly guideline 2.2 on user-centered design methods. Because most Americans vote no

more than once or twice per year, user-centered design is essential to provide systems that voters can use accurately and verifiably.

We believe that the guidelines should explicitly reference security as a crucial aspect of high-quality design. This can be accomplished by adding a new guideline 1.4, “Voting system design incorporates security best practices,” and by adding “best practices, including security best practices, in software development” in guideline 2.1.

Principle 3: Transparent

Guideline 3.1 refers to “security measures,” which ordinarily would refer to procedures rather than elements of voting system design. We suggest changing “security measures” to “security features.”

Principle 5: Equivalent and Consistent Voter Access

We support this principle. We recommend making explicit that guideline 5.1 extends to verification, for instance as follows: “Voters have a consistent experience throughout the voting process, including verification of the auditable records of their votes, in all modes of voting.” All voters deserve voting systems that facilitate verification.

Principle 6: Voter Privacy

We support this principle. We recommend revising guideline 6.2 to clarify, again, that the need for independent verification extends to whatever records will be used to audit tabulation accuracy. The phrase “ballot or other associated cast vote record” is too vague given the ambiguous definitions of both those terms. One possibility: “Voters can mark, verify and cast their ballot and other auditable records of their votes without assistance from others.”

Principle 7: Marked, Verified, and Cast as Intended

“Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.” We doubt that vote selections (contest selections?) can be cast. We believe the intended meaning is something like “Ballots, including contest options and contest selections, are presented in a perceivable, operable, and understandable way; ballots can be marked, verified, and cast by all voters.”

We recommend adding a guideline to the effect that “The voting system allows voters to consistently and accurately verify their ballots and the auditable records of their votes.” Such a guideline lends itself to requirements and test assertions that support high levels of voter verification. Here is another place where voting system security will largely depend on election procedures, such as polling place layout and the instructions given to voters.

Guideline 7.2 enigmatically specifies that “voters have direct control of all ballot changes.” The intended meaning may be “voters have direct control of all ~~ballot changes~~ changes in their contest selections.”

Principle 8: Robust, Safe, Usable, and Accessible

In guideline 8.3, “measuring... for effectiveness, efficiency, and satisfaction” seems vaguely defined. We recommend language that evokes a rigorous performance standard, such as “~~for effectiveness, efficiency, and satisfaction~~ accuracy, efficiency, and satisfaction in marking, verifying, and casting their ballots.”

Principle 9: Auditable

We recommend revising guideline 9.2 to underscore that vote records used to verify outcomes should also be voter-verified. Moreover, for the foreseeable future, we would require these records to be physical. Also, a “correct” election outcome is undefined. We suggest: “The voting system produces readily available physical records that voters could verify. These records provide the ability to check whether the election outcome corresponds with voters' contest selections and, to the extent possible, identify the root cause of any irregularities.”

In guideline 9.4, audit efficiency is desirable, but audit validity is paramount. We recommend expanding the guideline: “The voting system supports efficient, valid audits carried out with best practices.”

Principle 10: Ballot Secrecy

We agree with the comments of the Electronic Privacy Information Center (EPIC) in support of this principle. The term “ballot secrecy” is not included in the glossary, and its exact meaning is not self-evident: voted ballots themselves are not secret, and typically become public records once the election is complete. Verified Voting fully endorses the principle of ballot secrecy or ballot anonymity, as expressed in guideline 10.2: roughly, it should be impossible to tell how a particular person voted. We recommend defining this term in the glossary.

Principle 13: Data Protection

This principle, and guideline 13.4, appear to use “sensitive data” to refer both to data that should not be revealed due to privacy or confidentiality concerns, and data that is critical to the integrity of the election but not “sensitive” from a privacy standpoint. We suggest deleting “sensitive” from the principle (no data should be subject to “unauthorized access, modification, or deletion”), and drawing the distinction in guideline 13.4: for instance, “The voting system protects the integrity and authenticity of all data, and the confidentiality of sensitive data, transmitted over all networks.”

Principle 14: System Integrity

Guideline 14.2 appears to be missing a word: "...by reducing unnecessary code, data paths, and physical ports, and by using other technical controls." We further recommend replacing "reducing" with "avoiding" or "eschewing."

We concur with the recommendation of EPIC, the State Audit Working Group (SAWG), and others to add a new guideline (or add to 14.2): "The voting system does not use wireless technology or connect to any public telecommunications infrastructure." These risks are best eliminated.

In guideline 14.3, we concur with the SAWG proposal to insert: "The voting system maintains and verifies, and facilitates independent human verification of, the integrity of software, firmware, and other critical components." Systems should not be relied upon to verify themselves.

Principle 15: Detection and Monitoring

Guidelines 15.3 and 15.4 seem to go beyond the scope of the associated principle. It may be appropriate to add "prevention" to the principle or to narrow these guidelines, perhaps broadening guidelines associated with other principles accordingly.

About Verified Voting

Verified Voting (www.verifiedvoting.org), founded by computer scientists in 2004, is a leading national not-for-profit, non-partisan organization focused exclusively on the critical role technology plays in election administration. Through education and advocacy, our mission is to strengthen democracy by promoting the responsible use of technology in elections. Since our founding in 2004, we have acted on the belief that the integrity and strength of our democracy relies on citizens' trust that each vote is counted as cast. We bring together policymakers and officials who are designing and implementing voting-related legislation and regulations with technology and election administration experts who comprehend the risks associated with the emerging digital landscape, particularly the online and electronic elements in voting. Additionally, we connect advocates and researchers, the media and the public to provide greater understanding of these complex issues.

May 29, 2019

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Submitted electronically via votingsystemguidelines@eac.gov

Re: ACLU Comments on proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines (VVSG 2.0), 84 FR 6775

To Whom It May Concern:



Washington Legislative
Office
915 15th Street, 6th FL
Washington DC 20005
T: (202) 544-1681
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political
Director

The American Civil Liberties Union (ACLU) submits these comments in response to the request for public comment by the U.S. Election Assistance Commission (EAC) on the proposed Voluntary Voting System Guidelines 2.0 (VVSG 2.0) Principles and Guidelines.

The ACLU supports the newly proposed structure of the VVSG 2.0 of establishing high-level system design goals contained in the Principles and Guidelines followed by the separate development of more detailed documents addressing Requirements and Test Assertions. We believe this approach will provide greater clarity on operational and design goals that will assist with the development of voting systems moving forward.

The proposed Principles and Guidelines contain important principles that should be incorporated into the development of voting systems. We recommend the following standards to be included:

1. Free and Open Source Software Should be Standardized in Voting Systems

Free and open source software (FOSS) is a baseline software integrity measure that should be standardized in all voting systems used by the public in elections, and the ACLU strongly recommends its inclusion in the VVSG 2.0 Principles and Guidelines. Standardizing on FOSS will improve the integrity of our voting systems, and it has the additional benefit of enhancing public confidence in voting system security.

While we acknowledge FOSS is not necessarily the only way to achieve software accountability and is insufficient on its own to protect against cyber vulnerabilities, it is broadly understood as a starting point to securing software that requires the confidence of the general public. FOSS's advantages include public review, input, correction, and improvement of software. Accordingly, FOSS is accepted as a best practice in identifying and treating software

vulnerabilities, such as bugs, malware, and other potential susceptibilities independent of the vendor.

The alternative to FOSS is the continued use of proprietary software, which creates a number of disadvantages for elections administrators and the voting public. First, proprietary software forces election administrators into a dependent relationship with vendors; administrators are forced to accept the security safeguards offered by vendors and only receive software patches and updates when the vendor chooses to provide it. This has been a chronic problem for election administrators since transitioning voting systems as a result of the requirements of the Help America Vote Act (HAVA). Additionally, if a vendor discontinues a particular software program, an election administrator may be left with outdated, less secure software. The software running our elections should be accountable to the general public; that means it should be both auditable and fixable without being beholden to the vendor.

2. Improvements to Auditability Should Include Voter-Verifiable Paper Ballot Requirements for All Voting Systems

The Principles and Guidelines should incorporate a voter-verifiable paper ballot requirement for all voting systems. Voting systems must permit risk-limiting audits and therefore must have legible, human-interpretable audit trails. The goal should be that people, unaided by machines, can conceivably audit an election manually, and this requires a human-interpretable paper trail as a crucial check built into the voting systems we use in our elections.

3. Accessibility Standards for People with Disabilities and Language Minority Voters

The Principles and Guidelines should ensure that people with disabilities or who have limited mobility have access to voting at the same level that everyone else does. Accordingly, the Principles and Guidelines should include a standard that voting systems afford these voters a full and equal opportunity to cast their vote in private, and have their vote securely counted and included in any audit, privacy in the process of voting, ballot secrecy, and the same standard of convenience and time as able-bodied persons. We believe a voting system that meets this standard of accessibility and auditability is achievable through innovation and further development of current technology.

Similarly, the Principles and Guidelines should expressly address voting system standards that extend language minority voters full and equal access to the voting process. Under the coverage formula of Section 203 of the Voting Rights Act, the jurisdictions that must now provide non-English ballots and other elections materials encompass 68.8 million voting-age U.S. citizens. That represents 31.3% of the total U.S. voting-eligible population of 220 million.¹ It would be an enormous omission for this group of voters to be neglected in the standards of the Principles and Guidelines. While the Principles and Guidelines tacitly address accessibility and language access standards for these categories of voters in some of

¹ D'Vera Cohn, *More voters will have access to non-English ballots in the next election cycle*, Pew Research Center, (Dec. 16, 2016), available at <https://www.pewresearch.org/fact-tank/2016/12/16/more-voters-will-have-access-to-non-english-ballots-in-the-next-election-cycle/>.

the principles, the document should expressly and specifically set forth standards that meet at least these minimum requirements for these voting groups.

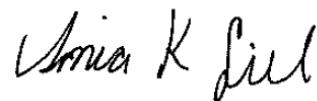
Conclusion

The ACLU understands the Principles and Guidelines are intended to provide high-level functionality goals for voting systems and strongly urge the foregoing items be included in this guiding document and further elaborated upon in the Requirements and Test Assertions documents. Please contact Sonia Gill, Senior Legislative Counsel, at sgill@aclu.org with any questions regarding this submission.

Sincerely,



Ronald Newman
National Political Director
National Political Advocacy Department



Sonia Gill
Senior Legislative Counsel
Washington Legislative Office



Daniel Kahn Gillmor
Senior Staff Technologist
Speech, Privacy, and Technology Project

June 7, 2019

To the Election Assistance Commission:

I welcome the new VVSG 2.0 as a significant improvement to the current voting system guidelines. However as drafted, the VVSG 2.0 provides inadequate security and will not be able to assure voters that their votes are being counted as cast. This may be due in part to reliance on the advice of voting system vendors, who have not historically shown a commitment to election security.

I ask that you make sure that all systems approved by the VVSG 2.0 meet the following standards:

NO APPROVED VOTING SYSTEM WILL :

1. allow Direct Record Electronic voting, even with a voter-verified paper audit trail. Studies have shown that voters do not verify paper audit trails from DRE machines and we need to move away from this system.
2. allow a ballot-marking device to act as a direct-record electronic system by allowing a vote to be recorded to computer memory or printed on a ballot without review by the voter - sometimes called "Permission to Cheat" mode."
3. have a modem, allow remote, wireless or internet access; or connect even incidentally to any computer or network that has been connected to a public network.
4. allow the technical opportunity for a machine to change a voter's selections on a ballot, after the voter has cast it – even if the machine is under the control of malware. It may be useful for some component of a voting system to print a unique identifier on a ballot, once the ballot is anonymous. But that capability must never allow voter selections to be impacted.
5. be a hybrid machine – with a printer and a scanner in the same path.
6. encode votes using barcodes or QR codes.
7. allow weighted election functions that use decimal counting methods. Votes must be counted as whole numbers.
8. allow "recallable ballot" provisions that enable the identification of a specific voter's ballot after it is cast. Once a ballot is recorded it must never be recallable.

ALL APPROVED VOTING SYSTEMS WILL

9. provide a durable paper ballot to be marked by hand by all voters who are capable. A paper ballot created by a machine is not sufficient.
10. provide accommodations for voters with disabilities that allow them to vote privately, independently and comfortably.
11. require testing and public opportunities for comment on all systems by voters with disabilities and disability advocates for a minimum of 45 days.

12. require testing and public opportunities for comment by the general public and independent security experts for a minimum of 45 day.
13. use durable paper known to retain a quality image for the 22 months required by HAVA, not thermal paper.
14. support the ability to have an accurate hand-counted audit of a trusted audit trail. An audit trail that can be compromised by a malware attack will not qualify as a trusted audit trail.
15. require that digital ballot images, cast vote records (CVRs), and the spreadsheets containing CVRs that are generated by digital scan voting systems will all be designated as "archival" public records that must be preserved for 22 months following a federal election. None of these items should be designated as "transient" materials.

The EAC must create a panel of technical election security experts, separate from NIST staff, with no financial relationship to vendors and no financial interest in emerging systems. The EAC needs to take input on the VVSG 2.0, and future policies from this panel - and other non-vested security experts on an ongoing basis. The EAC must stop its primary reliance on vendors and their representatives for technical guidance. This is a conflict of interest, and is undermining the ability of the EAC to create robust security protocols for our elections.

The EAC must set and meet the goal that by the end of 2022 40% of the Technical Guidance Development Committee will be made up of technologists and individuals with technology expertise.

Sincerely,
Andrea Flink

5/29/19

To the Election Assistance Commission:

We welcome the new VVSG 2.0 as a significant improvement to the current voting system guidelines. However as drafted, the VVSG 2.0 provides inadequate security and will not be able to assure voters that their votes are being counted as cast. Additionally, the drafting process has been flawed because it is too reliant on the biased input of voting system vendors, who have not historically shown a commitment to election security.

We ask that you make sure that all systems approved by the VVSG 2.0 meet the following standards:

NO APPROVED VOTING SYSTEM WILL:

1. record votes directly to a computer memory without the voter reviewing and verifying their selections on a paper ballot. The choices that are verified by the voter will be the choices used for tallying the votes.
2. have a modem, allow remote access or connect even incidentally to any computer, network, or network element that has been connected to a public network.
3. allow the technical opportunity for a machine to change a ballot, after the voter has cast it – even if the machine is under the control of malware.
4. be a hybrid machine – with a printer and a scanner in the same physical cabinet.
5. encode votes using barcodes, QR codes, or any other format that is not verifiable by a voter without assistive technology.
6. allow weighted election functions that use decimal counting methods. Votes must be counted as whole numbers.

ALL APPROVED VOTING SYSTEMS WILL

7. allow for the use of hand-marked paper ballots - not just a paper trail created by a machine, except for accommodations made for voters with disabilities.
8. use durable paper known to retain a quality image for the 22 months required by HAVA, not thermal paper.
9. support the ability to have an accurate hand-counted audit of a trusted audit trail. An audit trail that can be compromised by a malware attack will not qualify as a trusted audit trail.

FURTHER:

The EAC must create a panel of technical election security experts, separate from NIST staff, with no relationship to vendors and no vested interest in emerging systems. The EAC needs to take input on the VVSG 2.0, and future policies from this panel - and other non-vested security experts on an ongoing basis. The EAC must stop its primary reliance on vendors and their representatives for technical guidance. This is a conflict of interest, and is undermining the ability of the EAC to create robust security protocols for our elections.

(Affiliations are for identification purposes only and do not signify organizational endorsement.)

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
AND
U.S. TECHNOLOGY POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING
MACHINERY

to the
ELECTION ASSISTANCE COMMISSION

Notice of proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines request for public comment.

May 29, 2019

By notice published February 28, 2019, the Election Assistance Commission (“EAC”) requested public comment on the proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines (“VVSG 2.0”).¹

EPIC and the U.S. Technology Policy Committee of the Association for Computing Machinery (“USTPC”) support the proposed VVSG 2.0 and submit these comments to the EAC: (1) to commend the inclusion of strong principles protecting voter privacy, ballot secrecy, and data protection; and (2) to urge the Commission to include a ban on internet-connected voting machinery.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.² The Association for Computing Machinery is the longest-established and largest association of individual professionals engaged in all aspects of computing in the world.³ EPIC previously commented on the Voluntary Voting System Guidelines in 2009, stating:

Ballot secrecy and voter privacy must be core values within the context of voting technology standards and testing and certification of voting systems⁴

¹ Notice of proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines request for public comment, 84 Fed. Reg. 6775-76 (Feb. 28, 2019), <https://www.govinfo.gov/content/pkg/FR-2019-02-28/pdf/2019-03453.pdf>.

² EPIC, *About EPIC* (2018), <https://epic.org/epic/about.html>.

³ ACM engages in public policy through its U.S. Technology Policy Committee, to which participation in these comments should be attributed.

⁴ EPIC, Comments Regarding the 2009 Voluntary Voting System Guidelines Version 1.1, Election Assistance Commission, 6 (Sept. 28, 2009), https://epic.org/privacy/voting/epic_eac_comments_10-09.pdf.

I. The Secret Ballot is Vital for Democracy

We applaud the draft VVSG's robust principles on voter privacy and ballot secrecy. The secrecy of the ballot is a foundation of our democracy. In 2016, EPIC, Verified Voting, and Common Cause released a report and fifty state survey on the issue of ballot secrecy. We found that a vast majority of states (44) have a constitutional provision guaranteeing secrecy in voting, while the six remaining states have statutory provisions referencing secrecy in voting.⁵ The secret ballot is the kernel of democracy. "The secret ballot reduces the threat of coercion, vote buying and selling, and tampering. For individual voters, it provides the ability to exercise their right to vote without intimidation or retaliation."⁶

As the National Academy of Sciences recently found, "If anonymity is compromised, voters may not express their true preferences."⁷ While advances in technology can facilitate voting in a variety of ways—voter registration, tracking ballots, finding poll places, checking wait times, etc.—current cyber security techniques cannot prevent the linking of an individual to his or her marked ballot when transmitted over the internet.⁸ Thus digital voting techniques pose a real and ongoing risk in the specific area of vote tabulation.

EPIC and the USTPC urge the Commission to leave Principle 10: BALLOT SECRECY unchanged, ensuring that no direct or indirect identifiers can link the voter's identity with the "voter's intent, choices, or selections."⁹

II. Algorithmic Transparency is Key to Ensuring Accountability

Accountability is key to ensuring faith in our electoral process. As decisions are automated, and organizations increasingly delegate decision-making to techniques they do not fully understand, processes become more opaque and less accountable. It is therefore imperative that algorithmic process be open, provable, and accountable.

We commend the inclusion of guideline 13.3 – "All cryptographic algorithms are public, well-vetted, and standardized" and urge the Commission to leave the guideline unchanged.

III. The VVSG 2.0 must ban internet connectivity or the use of wireless modems in voting systems

The VVSG 2.0 draft is missing a requirement that is critical to election security: a ban on internet connectivity or the use of wireless modems in vote recording or vote tabulating systems. The current draft would allow voting machines to connect to the Internet, perhaps even through a wireless connection.

⁵ Caitriona Fitzgerald, Pamela Smith, Susannah Goodman, *Secret Ballot at Risk: Recommendations for Protecting Democracy*, 1 (Aug. 18, 2016), <http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf>.

⁶ *Id.* at 5.

⁷ National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* 87 (2018), <https://doi.org/10.17226/25120>.

⁸ *Id.* at 4.

⁹ Proposed Voluntary Voting System Guidelines 2.0 Principles and Guidelines at 4.

We urge the Commission to add a guideline under Principle 13: DATA PROTECTION:

"The voting system does not use wireless technology or connect to any public telecommunications infrastructure."

As the National Academies of Sciences, Engineering, and Medicine stated in the 2018 Report on election security:

At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.¹⁰

The National Academies concluded that “[s]ecure Internet voting will likely not be feasible in the near future.”¹¹

Computer scientists have long cautioned that Internet voting “not only entails serious security risks, but also requires voters to relinquish their right to a secret ballot.”¹² After the 2016 election, cybersecurity expert Bruce Schneier wrote:

We need national security standards for voting machines, and funding for states to procure machines that comply with those standards.

This means no Internet voting. While that seems attractive, and certainly a way technology can improve voting, we don’t know how to do that securely. We simply can’t build an Internet voting system that is secure against hacking because of the requirement for a secret ballot. This makes voting different from banking and anything else we do on the Internet, and it makes security much harder. Even allegations of vote hacking would be enough to undermine confidence in the system, and we simply cannot afford that.¹³

¹⁰ National Academies of Sciences, Engineering, and Medicine, *supra* note 7, at 106.

¹¹ *Id.* at 102.

¹² Douglas W. Jones and Barbara Simons, *Broken Ballots: Will Your Vote Count?* 291 (2012); Bruce Schneier, *By November, Russian hackers could target voting machines*, Washington Post (July 27, 2016), <https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/>; *Accord* Verified Voting, Computer Technologists’ Statement on Internet Voting (September 2012), <http://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf>; see also Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold Accuvote-Ts Voting Machine Problems with Voting Systems and the Applicable Standards* (Sept. 2006), <https://citp.princeton.edu/research/voting/>; Peter G. Neumann, Security Criteria for Electronic Voting (1993), available at <http://www.csl.sri.com/users/neumann/ncs93.html>.

¹³ Bruce Schneier, *Online Voting Won’t Save Democracy*, The Atlantic (May 2017), <https://www.theatlantic.com/technology/archive/2017/05/online-voting-wont-save-democracy/524019/>.

Renowned cryptographer Ronald Rivest says that “best practices for internet voting are like best practices for drunk driving.” – neither one makes sense.¹⁴ Rivest says the dramatic loss of security with Internet voting does not outweigh the increased convenience for voters.¹⁵

Cyber security experts at the Department of Homeland Security and the National Institutes for Standards and Technology have warned against implementation of Internet voting in U.S. public elections because of privacy and security risks.¹⁶ In July 2015, the U.S. Vote Foundation released a study establishing a new reference for security, usability and transparency standards necessary to implement Internet voting in public elections. Developed by the nation’s leading experts in election integrity, election administration, high-assurance systems engineering, and cryptography, the study concluded that **not one** of the existing Internet voting systems provides adequate security for public elections or guarantees voter privacy.¹⁷

Washington DC’s Internet voting pilot system was allowed to be tested before deployment. Researchers breached it with relative ease: “Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters’ secret ballot.”¹⁸

Cybersecurity must be a top priority for the United States. We must protect democratic institutions against cyber attack by foreign adversaries. The Russian attacks on democratic institutions are expected to continue.¹⁹ As the National Academies of Sciences, Engineering, and Medicine recently explained:

The 2016 election vividly illustrated that hostile state actors can also pose a threat. These actors often possess more sophisticated capabilities and can apply greater resources to the conduct of such operations. Moreover, they may have other goals than shifting the outcome for a particular candidate. If their goal is to disrupt an election or undermine confidence in its outcome, they may need only to achieve DoS against e-pollbooks or leave behind traces of interference like malicious software or evidence of tampering with voter registration lists or other records. Even failed attempts at

¹⁴ Christine Kane, *Voting and Verifiability: Interview with Ron Rivest*, Vantage Magazine (2010), <https://people.csail.mit.edu/rivest/pubs/Kan10.pdf>

¹⁵ *Id.*; see also Ron Rivest, Auditability and Verifiability of Elections (March 2016), available at <https://people.csail.mit.edu/rivest/pubs/Riv16x.pdf>.

¹⁶ Sari Horwitz, *More than 30 states offer online voting, but experts warn it isn’t secure*, Wash. Post (May 17, 2016), available at <https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/>; see also National Institute of Standards and Technology (NIST), *Security Considerations for Remote Electronic UOCAVA Voting* (February 2011), available at <http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf>; and Federal Voting Assistance Program, *2010 Electronic Voting Support Wizard (EVSW) Technology Pilot Program Report to Congress* (May 2013), available at http://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf.

¹⁷ U.S. Vote Foundation, *The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study* (July 2015), available at <https://www.usvotefoundation.org/E2E-VIV>.

¹⁸ Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, *Attacking the Washington, D.C. Internet Voting System*, Proc. 16th Conference on Financial Cryptography & Data Security (Feb. 2012), <https://jhalderm.com/pub/papers/devoting-fc12.pdf>.

¹⁹ Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (2017), 5, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

interference could, if detected, cast doubt on the validity of election results absent robust mechanisms to detect and recover from such attacks.²⁰

The VVSG help shape the election security market. The Election Assistance Commission should not miss this critical opportunity to make a strong statement that elections and the Internet don't mix. The VVSG should add a guideline that bans internet connectivity or the use of wireless modems in vote recording or vote tabulating systems.

Conclusion

The VVSG 2.0 are vital to protecting our democratic institutions. The guidelines must ban the use of internet-connected voting machines and protect ballot secrecy.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

James A. Hendler
Chair, U.S. Technology Policy Committee of
the Association for Computing Machinery

²⁰ National Academies of Sciences, Engineering, and Medicine, *supra* note 7, at 92.



Advancing the human and civil rights of people with disabilities

SELF-ADVOCACY ASSISTANCE ★ LEGAL SERVICES ★ DISABILITY RIGHTS EDUCATION ★ PUBLIC POLICY ADVOCACY ★ ABUSE INVESTIGATIONS

May 29, 2019

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Equip for Equality's Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

Equip for Equality, the federally mandated non-profit organization designated as the Protection and Advocacy (P&A) agency for individuals with disabilities in Illinois, appreciates the opportunity to comment on the draft Voluntary Voting System Guidelines 2.0. Principles and Guidelines. The P&A system was established by the U.S. Congress to protect the rights of people with disabilities and their families through legal support, advocacy, referral, and education. P&As are in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Territories (American Samoa, Guam, Northern Mariana Islands, and the US Virgin Islands), and there is a P&A affiliated with the Native American Consortium, which includes the Hopi, Navaho and San Juan Southern Paiute Nations in the Four Corners region of the Southwest. Together, the P&A network is the largest provider of legally based advocacy services to people with disabilities in the U.S. Through the Protection and Advocacy for Voter Access (PAVA) program, created by the Help America Vote Act of 2002, the P&As have a federal mandate to "ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places" and are the leading expert on access to the vote for people with disabilities in the U.S.

Equip for Equality commends the U.S. Election Assistance Commission (EAC) for its efforts to balance election security with federal elections accessibility requirements under law. However, Equip for Equality is concerned that the only voting systems capable of meeting VVSG 2.0's requirements will be reliant on a marked paper ballot as the ballot of record, a concern that has been further confirmed by the technical standards for the VVSG that are currently being developed in public forums. We acknowledge that the promise of fully accessible, paper-based voting systems has existed since the passage of HAVA. Yet, the hope that paper ballots will be made accessible, private and able to be cast independently, for people with disabilities is not now, and may never be, a reality. Widespread implementation of market-ready, fully accessible paper ballot voting systems is simply not achievable in the foreseeable future.

THE INDEPENDENT, FEDERALLY MANDATED PROTECTION & ADVOCACY SYSTEM FOR THE STATE OF ILLINOIS

JOHN K. HOLTON, Ph.D., BOARD CHAIRPERSON ZENA NAIDITCH, PRESIDENT & CEO

1 WEST OLD STATE CAPITOL PLAZA ★ SUITE 816 ★ SPRINGFIELD, IL 62701 ★ EMAIL: CONTACTUS@EQUIPFOREQUALITY.ORG

TEL: (217) 544-0464 ★ TOLL FREE: (800) 758-0464 ★ TTY: (800) 610-2779 ★ FAX: (217) 523-0720 ★ MULTIPLE LANGUAGE SERVICES

WWW.EQUIPFOREQUALITY.ORG

Further, VVSG 2.0 is premised upon the out-dated concept of “one accessible system per polling place.” The assumption that voting accessibility is limited to use of a ballot marking system at a traditional polling place ignores the rapidly expanding opportunities to participate in the electoral process outside casting a ballot at one’s polling place on Election Day. Increasingly, voters with disabilities and their non-disabled peers are availing themselves of opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the extent of the VVSG’s reach into non-traditional voting systems.

Equip for Equality believes that the failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated electoral processes restrict any voter that benefits from use of the accessible voting system to a separate line, while other voters hand mark their paper ballots. Segregated systems are a form of discrimination and inherently unequal and should no longer be considered a standard, acceptable practice in the U.S. The assumption that a majority of voters will hand mark their ballots means that there are a limited number of accessible voting machines present. Poll workers are inadequately trained to operate them. As a result, poll workers at their best are unable to describe and activate accessibility features included in the equipment’s design. At worst, poll workers discourage use of the equipment by voters or leave the voting machine turned off, still in it’s case, and even hidden from view. For the voters that are able to cast their ballots on the one accessible system available, the secrecy of their ballots cannot be guaranteed. The ballots often vary in appearance from hand marked ballots and may even be counted and stored separately. Disappointingly, the accessibility ratios/quotas (similar to calculating the number of accessible parking spaces required based on the size of a parking lot) and requirements that electronic voting technology produce a comparable ballot to those hand marked are outside the scope of the VVSG.

While Equip for Equality believes that U.S. elections must be accurate and understands the intent to address cyber security issues, the VVSG is widely used by voting technology manufacturers to guide the development of their products and by state and local elections officials to inform purchase and implementation of voting equipment. In undertaking this process of a comprehensive re-envisioning of the guidelines, the EAC should expand the VVSG’s scope to encompass all technology used to cast ballots within or beyond the traditional polling place. Further, the VVSG must ensure a private and independent ballot for all voters in a fully integrated experience that respects the dignity of the voter and the secrecy of the ballot.

May 29, 2019

Page 3

Thank you for the opportunity to comment on this important set of principles and guidelines. If you have any questions please feel free to contact me at 217-303-8543 or cherylj2@equipforequality.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Cheryl R. Jansen".

Cheryl R. Jansen

Public Policy Director



May 28, 2019

US Election Assistance Commission (EAC)
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Commissioner Christy McCormick, Chairwoman
Commissioner Benjamin W. Hovland, Vice Chair
Commissioner Donald L. Palmer
Commissioner Thomas Hicks

Re: EAC Voluntary Voting System Guidelines 2.0 Principles and Guidelines Comments

Dear Commissioners McCormick, Hovland, Palmer and Hicks:

Election Systems & Software (ES&S) respectfully submits this letter and attached set of comments for consideration and inclusion into the public comments for the EAC Voluntary Voting System Guidelines 2.0 Principles and Guidelines adopted on February 15, 2019.

The Principles and Guidelines are a tremendous step toward accomplishing this goal, but on their own, manufacturers cannot begin the design and development steps to produce 2.0 compliant voting systems. It is essential for the full set of detailed requirements and associated test assertions to be completed and approved for us to incorporate into our 2.0 development.

ES&S offers our appreciation and full support to the EAC in the completion of the Voluntary Voting System Guidelines 2.0 and we will continue to work with you up to and through their final adoption.

Please do not hesitate to contact us if we can provide any further clarity or respond to questions.

Respectfully,

A handwritten signature in blue ink that reads "Steve M. Pearson".

Steve M. Pearson
SVP, Certification

Attachment: ES&S VVSG 2.0 Principle & Guideline Comments, May 28, 2019

ES&S VVSG 2.0 Principle & Guideline Comments

May 28, 2019

1. Principle 1: High Quality Design

- 1.1. Are commonly accepted election process specifications generally agreed to and documented for reference?
- 1.2. Does VSTL testing validate real world operating conditions?
- 1.3. What evaluation methods are anticipated to be used? What is meant by specified properties?

2. Principle 2: High Quality Implementation

- 2.1. What trustworthy materials are being referenced? There are many different software development practices that can be referred to as best practices. Will any standard process be accepted?
- 2.2.
- 2.3. How will the voting system logic be assessed to determine if it is clear, meaningful and well-structured? What is the definition of clear, meaningful and well structured?
- 2.4. How will the voting system be assessed to determine if it is modular, scalable and robust? What is the definition of modular, scalable and robust?
- 2.5. How is integrity defined? Does integrity refer to security?
- 2.6. Does this refer to the EMS, voting machines or tabulation equipment? Or perhaps all of these components?
- 2.7. Does VSTL testing validate reliable performance in anticipated physical environments?

3. Principle 3: Transparent

- 3.1. What specific design documents are being referred to? Is it similar the currently accepted TDP?
- 3.2. What does this really mean? Readily available for what kind of inspection? Code review? Log review? This guideline needs further clarification.
- 3.3. Is this accomplished by L&A testing, ballot review, or through a public documented and verified description of the ballot handling from voted ballots through the final certified results?

4. Principle 4: Interoperable

- 4.1. Does imported/exported mean data moving outside of the jurisdiction's voting ecosystem? Has an interoperable format been defined?
- 4.2. Do publicly available formats refer to the NIST standard formats? Others?
- 4.3.
- 4.4. Are COTS devices subject to the same level of examination for security, accuracy, reliability, and safety as purpose built voting system components?

5. Principle 5: Equivalent and Consistent Voter Access

- 5.1. Does this imply that all voters (ADA and non-ADA) are required use the same method for voting?
- 5.2. Can this equivalent information be in a different form and format?

6. Principle 6: Voter Privacy

- 6.1.
- 6.2.

7. Principle 7: Marked, Verified and Cast as Intended

- 7.1.
- 7.2. What is meant by ballot changes? Contest selections? Other?

7.3.

8. Principle 8: Robust, Safe, Usable, and Accessible

- 8.1. What is the definition of harmful conditions? Do they include both physical and logical conditions?
- 8.2.
- 8.3. Does measured mean tested with a wide range of voters? What are the parameters for measurement?
- 8.4.

9. Principle 9: Auditable

- 9.1. What is the definition of an error or a fault?
- 9.2. Does this refer to both electronic and paper records?
- 9.3. What is the definition of resilient? Does it include encryption and redundancy?
- 9.4. Does efficient mean RLAs? How will efficient be measured?

10. Principle 10: Ballot Secrecy

- 10.1.
- 10.2.

11. Principle 11: Access Control

- 11.1. This seems to be partially procedural for jurisdictions to implement. How does this apply to voting systems?
- 11.2. This seems to be partially procedural for jurisdictions to implement. How does this apply to voting systems?
- 11.3. How broadly does multi-factor authentication need to be applied? How is “strong” defined and measured?
- 11.4.
- 11.5.

12. Principle 12: Physical Security

- 12.1. What are mechanisms? Do they include both physical and logical mechanisms?
- 12.2.

13. Principle 13: Data Protection

- 13.1. How is this different from section 11? Is this intended to prevent users with valid access from tampering with critical files such as CVR's and audit data?
- 13.2.
- 13.3.
- 13.4. What is sensitive data?

14. Principle 14: System Integrity

- 14.1. How is this different from 13.4?
- 14.2. What is included in other technical controls?
- 14.3. Is this referring to validation of installed firmware/software and prevention/detection of any modification?
Supply chain management?
- 14.4.

15. Principle 15: Detection and Monitoring

- 15.1. What are the automated processing requirements?
- 15.2.
- 15.3. What is included in mechanisms? Does it encompass hardware, software and human controls?
- 15.4. How are best practices defined?

General Comments:

1. How will the 2.0 guidelines reference the 1.1 guidelines?
2. Will the 2.0 requirements be built on the 1.1 guidelines?
3. What level of specificity will be included in the 2.0 guidelines?
4. Clear, concise, and testable Requirements and associated Test Assertions are required for manufacturers to begin development toward 2.0 compliant voting systems.
5. What are the review and approval processes for the Requirements and Test Assertions?
6. What is the timing for approved Requirements and Test Assertions?



May 29, 2019

Submitted Electronically

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Re: Comments on EAC VVSG 2.0 of the U.S. Technology Policy Committee of the Association for Computing Machinery

Dear Chairwoman McCormick:

The Association for Computing Machinery (“ACM”) is the longest established and, with more than 100,000 global members, the largest association of individual professionals engaged in all aspects of computing in the world. A non-lobbying and otherwise wholly apolitical organization, ACM’s mission includes providing unbiased, expert technical advice to policy-makers on matters of our members’ wide-ranging expertise. That work is accomplished in the United States by and through ACM’s U.S. Technology Policy Committee (the “Committee”).

The Committee commends the Commission for opening this proceeding to refine the second iteration of its Voluntary Voting System Guidelines (“VVSG 2.0”) and, consistent with our mandate, is pleased to again¹ have the opportunity to assist the Election Assistance Commission. We look forward to future opportunities to comment in greater technical detail upon the means of implementing the high-level principles and guidelines that are currently (and we believe productively) the focus of this stage of the proceeding. For present purposes, the Committee wishes to:

¹ Committee member David Wagner leads the security team of the EAC’s Technical Guidelines Development Committee (TGDC) on which Committee member Ron Rivest and Vice Chair Jeremy Epstein also previously sat. Epstein also served as a panelist at the EAC’s January 10, 2018 Summit on the 2018 election.

- associate itself with select comments, detailed in the attached matrix, of several other respected civil society organizations,² as well as with specific points made in the individual filing of Dr. Philip Stark;
- clearly underscore that, to be as secure and verifiable as possible, *all* voting technology must be: ***isolatable*** from inherently vulnerable networks of all kinds; ***inspectable*** with very high confidence at every stage of operation; and ***interoperable*** to maximize efficiency and system modernity.

The Committee thus specifically and emphatically recommends that the final VVSG:

1. **Endorse a blanket ban on the internet connection capability of any and every voting technology addressed by the VVSG, *including connection to any private network that ultimately may connect to the internet*.** This categorical prohibition on the inclusion of any connectivity-enabling devices in election-related equipment include all wireless modems, radios, and any other type of equipment capable of communicating over the internet. *Simply disabling such devices if installed will not suffice to protect election networks, databases and equipment.*
2. **Foster and justify public confidence that our election results are wholly evidence-based by requiring that elections be fully and robustly auditible.** To accomplish this goal, *all post-election ballot audits must occur before results are finalized and certified.* Moreover, such universal post-election assessment must include both *compliance audits* that verify the audit trail and *risk-limiting* ballot audits that either validate the declared results or determine what the correct results should be.
3. **Require the full interoperability of all internal voting system components, peripherals and data formats, together with component and system integration testing and certification.** Component testing would significantly decrease vendor development and testing costs. Component certification, combined with interoperability, almost certainly would decrease the costs and increase the options of election officials by facilitating the modular replacement of only those portions of their systems that require upgrading rather than systems in their entirety, as is now the norm. Component testing also would lower the barriers to market entry for new and potentially innovative component-producing companies which would be relieved from the present burdens of having to develop complete election systems.

² The Committee has carefully reviewed and emphasizes in the attached Appendix select observations and recommendations of the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), and Verified Voting (VV).

Thank you again for the opportunity to participate in this critical effort. Should you or your staff have any questions regarding these Comments, or seek further expert analysis or information our members may provide, please email Adam Eisgrau, ACM's Washington-based Director of Global Policy & Public Affairs, at the address below or reach him at 202-580-6555.

Sincerely,



James A. Hendler, Chair

Appendix

**ASSOCIATION FOR COMPUTING MACHINERY
U.S. TECHNOLOGY POLICY COMMITTEE COMMENTS ON EAC VVSG 2.0
ADDITIONAL CONCEPTS AND COMMENTS ENDORSED**

ACM's U.S. Technology Policy Committee also makes the following additional general points (unattributed) and associates itself with the specific analyses of VVSG 2.0 identified below articulated variously in their Comments by: the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), Verified Voting (VV), and Dr. Philip Stark (PS).

Principle	Issue	Comment/Analysis	Source(s)
General	Structure	<ul style="list-style-type: none">▪ Separation of proposed principles from detailed technical requirements.	PS
General	Process	<ul style="list-style-type: none">▪ Approval of technical requirements and test assertions without EAC vote.	VV
General	Objective	<ul style="list-style-type: none">▪ VVSG must: "deliver meaningful and effective guidance and requirements that will improve the security of voting systems and lessen exposure to manipulation, tampering or hacking."	NEDC
General	Auditability	<ul style="list-style-type: none">▪ Our nation must conduct and verify fully auditable evidence-based elections.	PS, SAWG, VV
General	Connectivity	<ul style="list-style-type: none">▪ No device involved in balloting or election administration should be connected <i>or connectable</i> to the internet or any private network that connects to the internet.	EPIC, NEDC, PS
4	Interoperability	<ul style="list-style-type: none">▪ Strongly supported for all devices and data.	
5	Voter Access	<ul style="list-style-type: none">▪ Voters must have equal and consistent access to election systems and resources.	
6	Voter Privacy	<ul style="list-style-type: none">▪ Voter privacy must be assured and protected in all phases of the election process.	
7	Balloting	<ul style="list-style-type: none">▪ Ballot text, form and vote selections must be presented in a clear and understandable way that can easily be marked and verified by all voters.▪ Voting systems must allow voters to consistently and accurately verify both their ballots and the auditable records of their votes.▪ Voters with disabilities must be able to independently validate their ballots.	VV PS

8	Voting Systems/ Processes	<ul style="list-style-type: none"> ▪ Voting systems and processes must be “robust, safe, usable and accessible. ▪ 8.3: System accuracy and ease of use must be prioritized over voter “satisfaction.” 	PS
9	Auditability	<ul style="list-style-type: none"> ▪ 9.2: Election/voting records must be verifiable by the voter. 	VV
10	Ballot Secrecy	<ul style="list-style-type: none"> ▪ It should not be possible to link the voter to his or her ballot once the ballot has been cast. ▪ “Voters should vote privately . . . but votes should [more accurately] be [considered and described as] anonymous rather than secret.” ▪ Delete “recallable ballot” from the glossary as the notion of a recallable ballot inherently conflicts with a ballot secret and anonymity. 	EPIC PS SAWG
13	Data Protection	<ul style="list-style-type: none"> ▪ Add a separate guideline articulating the clear prohibition on internet “connectivity,” above. 	NEDC
15	Detection and Monitoring	<ul style="list-style-type: none"> ▪ 15.4: As this provision presumes the interconnection of voting systems with the internet or other networks in contravention of the recommended prohibition, it should be eliminated. 	PS
Glossary		<p>The Committee also concurs that the following key Glossary terms should be added or modified:</p> <ul style="list-style-type: none"> ▪ Audit ▪ Ballot ▪ Ballot Secrecy ▪ Ballot Selections ▪ Cast Vote Record ▪ Correct (re: election outcomes) ▪ Effectiveness ▪ Efficiency ▪ Resilience ▪ Sensitive Data ▪ Voter Selections 	PS PS, VV SAWG, VV SAWG PS, SAWG, VV VV PS PS SAWG VV SAWG



June 6, 2019

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland

Submitted electronically

RE: Proposed Voluntary Voting Standard Guidelines (VVSG) 2.0
84 Fed. Reg. 6,775 (Feb. 28, 2019)

Dear Chairwoman McCormick:

We write to comment on the Proposed Voluntary Voting Standard Guidelines (VVSG) 2.0. Free Speech for People (FSFP) is a national, non-profit, non-partisan organization that works to fight for free and fair elections in a democratic process in which all people have an equal voice and an equal vote. National Election Defense Coalition (NEDC) is a non-partisan non-profit project organized that aims to promote secure, reliable, and transparent elections.¹

We request the addition of a provision sunsetting VVSG 1.0 and 1.1. The Testing Manual currently allows for the manufacturer of a voting system to choose the VVSG to which the manufacturer wishes to have the system tested and certified. *See EAC, Testing and Certification Program Manual, version 2.0* (May 31, 2015), § 4.3.1.3.²

The world of technology has changed significantly since 2005, when VVSG 1.0 was established: the iPhone had not yet been released, and Facebook was still “The Facebook” and only available to college students. We are concerned that

¹ NEDC previously submitted comments on the proposed VVSG 2.0, dated May 29, 2019. This comment is supplemental to that earlier comment. FSFP adopts NEDC’s May 29, 2019 comment in addition to this comment.

² <https://www.eac.gov/assets/1/28/Cert.Manual.4.1.15.FINAL.pdf>

allowing earlier VVSGs to remain available will allow manufacturers to obtain certifications in conformity with 2005 standards, which do not reflect modern expectations of a voting machine (or indeed any computer) with respect to usability, reliability, and security.

This concern is evidenced by the fact that even after VVSG 1.1 was promulgated in 2015, voting systems manufacturers have continued to request their systems be tested and certified against VVSG 1.0, such as the EVS 6.0.0.0 from ES&S, certified on July 2, 2018. The EAC should not permit manufacturers to continue to test and certify against older versions of the VVSG once version 2.0 has been finalized.

Thank you for the opportunity to comment on the Guidelines.

Sincerely,

Ronald Fein, Legal Director
Free Speech For People
617-244-0234
rfein@freespeechforpeople.org

Susan Greenhalgh, Policy Director
National Election Defense Coalition
917-796-8782
susan@electiondefense.org



June 6, 2019

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland

Submitted electronically

RE: Proposed Voluntary Voting Standard Guidelines (VVSG) 2.0
84 Fed. Reg. 6,775 (Feb. 28, 2019)

Dear Chairwoman McCormick:

We write to comment on the Proposed Voluntary Voting Standard Guidelines (VVSG) 2.0. Free Speech for People (FSFP) is a national, non-profit, non-partisan organization that works to fight for free and fair elections in a democratic process in which all people have an equal voice and an equal vote. National Election Defense Coalition (NEDC) is a non-partisan non-profit project organized that aims to promote secure, reliable, and transparent elections.¹

We request the addition of a provision sunsetting VVSG 1.0 and 1.1. The Testing Manual currently allows for the manufacturer of a voting system to choose the VVSG to which the manufacturer wishes to have the system tested and certified. *See EAC, Testing and Certification Program Manual, version 2.0* (May 31, 2015), § 4.3.1.3.²

The world of technology has changed significantly since 2005, when VVSG 1.0 was established: the iPhone had not yet been released, and Facebook was still “The Facebook” and only available to college students. We are concerned that

¹ NEDC previously submitted comments on the proposed VVSG 2.0, dated May 29, 2019. This comment is supplemental to that earlier comment. FSFP adopts NEDC’s May 29, 2019 comment in addition to this comment.

² <https://www.eac.gov/assets/1/28/Cert.Manual.4.1.15.FINAL.pdf>

allowing earlier VVSGs to remain available will allow manufacturers to obtain certifications in conformity with 2005 standards, which do not reflect modern expectations of a voting machine (or indeed any computer) with respect to usability, reliability, and security.

This concern is evidenced by the fact that even after VVSG 1.1 was promulgated in 2015, voting systems manufacturers have continued to request their systems be tested and certified against VVSG 1.0, such as the EVS 6.0.0.0 from ES&S, certified on July 2, 2018. The EAC should not permit manufacturers to continue to test and certify against older versions of the VVSG once version 2.0 has been finalized.

Thank you for the opportunity to comment on the Guidelines.

Sincerely,

Ronald Fein, Legal Director
Free Speech For People
617-244-0234
rfein@freespeechforpeople.org

Susan Greenhalgh, Policy Director
National Election Defense Coalition
917-796-8782
susan@electiondefense.org



ELECTION ASSISTANCE COMMISSION (EAC)

TOPIC: VVSG 2.0 PRINCIPLES & GUIDELINES

Date: May 28, 2019

HART COMMENTS

Hart InterCivic, Inc. is committed to election integrity and is proud of the role we play in the election technology space. We want to thank the US Election Assistance Commission (EAC) for playing a vital role in setting a single federal standard for the testing and certification of election devices and software. Your work is a considerable asset to both the vendors who manufacture election systems and the government officials who deploy them.

As a leading election system manufacturer, Hart's ability to bring new, innovative products and timely upgrades to market is strained and slowed by a lengthy federal certification process. We are very encouraged to hear the EAC has increased its certification team staff back to three full-time employees, and we will continue to implore Congress to give the agency the resources needed to further staff up.

As the EAC moves forward to approve and eventually release the full VVSG 2.0 – including the technical requirements and test assertions that interpret and direct the specifications of system builds – we strongly encourage you to find a balance between the requirements that direct policy choices and should be approved by Commissioners, and those that direct technical builds and may be appropriate for approval and updates by EAC career staff through a clearly defined and mapped process that takes in feedback from appropriate stakeholders such as the EAC's Advisory Board, the vendors who build systems, and the VSTLs that test them.

The country cannot go another decade without updates to the only federal standards for election equipment. However, a system with unfettered updates coming without a strict and transparent approval process that requires feedback from key stakeholders would be equally problematic. We know it will be no small task to develop a system to allow for limited approval of recommendations and test assertions by EAC staff, but such a hybrid system could drastically improve the security posture of our national election system.

Hart's comments on the VVSG 2.0 Principles and Guidelines are embedded in red in the pages that follow.

Voluntary Voting System Guidelines 2.0

Principles and Guidelines

Principle 1: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly-accepted election process specifications.

Hart Comment: How will the EAC interpret the phrase “commonly-accepted” specifications? Is this a reference to federal and state certification processes? If so, state that more directly.

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

Principle 2: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

Hart Comment: The word “trustworthy” is subjective and often loaded with subjective connotation. Whose “trust” will set the standard?

2.1 seemingly refers to supply chain best practices. If that is the case, state that directly.

Whose “best practices?” For example, does this refer to the EAC? DHS? CIS? And what will the process be to update old best practices as technology and voting behavior changes?

2.2 - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

Hart Comment: “Modular” seems out of place in a section on implementation. Is “extendable” a more applicable term here than “modular?”

2.5 - The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in anticipated physical environments.

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Hart Comment: 3.3. seems to apply to public trust in the system. But is this Principle really about audits? If so, state that more directly.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly-available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Hart Comment: There may be a challenge in implementing 4.4 because many of the best COTS devices cannot meet VVSG standards (they were never designed for that purpose).

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities, without discrimination.

5.1 - Voters have a consistent experience throughout the voting process in all modes of voting.

Hart Comment: Hart suggests striking “consistent” and replacing it with “equivalent.” Voters with disabilities may receive *more* information/assistance than able-bodied voters.

5.2 - Voters receive equivalent information and options in all modes of voting.

Hart Comment: Same comments as 5.1 – “consistent” is not really accurate and could therefore create unintentional problems.

Principle 6: VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

Hart Comment: There is no way around the fact that a small percentage of voters will not be able to cast a ballot truly "independently," no matter the system – some degree of assistance will be necessary.

How do we square that reality with the wording of 6.2?

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware and accessories protect users from harmful conditions.

Hart Comment: "Protect" may not be the best word to convey this concept. Hart suggests: "...should not expose voters to harmful conditions."

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 The voting system is evaluated for usability by election workers.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

Hart Comment: The term “evidence-based” is open-ended and subjective. This is an instance where more specificity would improve the Principle. What constitutes “evidence,” and who decides what is or is not “evidence?”

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

Hart Comment: What processes for checking (validating) the outcome of an election are envisioned here? 9.2 is overly broad and should be refined with more detail.

Does 9.2 imply a requirement for a printed paper ballot?

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

Hart Comment: The wording here creates unintended confusion: how can a system be resilient to “accidental” errors? Does 9.3 mandate encryption? If so, state that more directly.

Voting system records must be protected both physically and by process (e.g. audit logs). That point isn’t made clear in Principle 9.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters’ ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.

Hart Comment: There are two cases that may clash with the specific wording in 10.2: 1) provisional ballots, and 2) state-mandated voidable ballots.

If Principle 10 clashes with state cert guidelines, this could become a serious challenge for vendors to pass state testing and certification programs.

Hart suggests an exception clause – “...except for provisional voting and state-mandated voidable ballots.”

Principle 11: ACCESS CONTROL

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION

The voting system protects sensitive data from unauthorized access, modification, or deletion.

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

Hart Comment: “Sensitive” is too broad and open to competing interpretations for a topic this important. Even with additional supporting information coming in the regulations and test assertions, 13.4 should better define the data it is trying to protect.

It is very possible that data which some would identify as “sensitive” is necessarily released for important reasons of transparency or auditability.



Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

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

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system employs mechanisms to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.



May 29, 2019

Submitted Electronically

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Re: Comments on EAC VVSG 2.0 of the U.S. Technology Policy Committee of the Association for Computing Machinery

Dear Chairwoman McCormick:

The Association for Computing Machinery (“ACM”) is the longest established and, with more than 100,000 global members, the largest association of individual professionals engaged in all aspects of computing in the world. A non-lobbying and otherwise wholly apolitical organization, ACM’s mission includes providing unbiased, expert technical advice to policy-makers on matters of our members’ wide-ranging expertise. That work is accomplished in the United States by and through ACM’s U.S. Technology Policy Committee (the “Committee”).

The Committee commends the Commission for opening this proceeding to refine the second iteration of its Voluntary Voting System Guidelines (“VVSG 2.0”) and, consistent with our mandate, is pleased to again¹ have the opportunity to assist the Election Assistance Commission. We look forward to future opportunities to comment in greater technical detail upon the means of implementing the high-level principles and guidelines that are currently (and we believe productively) the focus of this stage of the proceeding. For present purposes, the Committee wishes to:

¹ Committee member David Wagner leads the security team of the EAC’s Technical Guidelines Development Committee (TGDC) on which Committee member Ron Rivest and Vice Chair Jeremy Epstein also previously sat. Epstein also served as a panelist at the EAC’s January 10, 2018 Summit on the 2018 election.

- associate itself with select comments, detailed in the attached matrix, of several other respected civil society organizations,² as well as with specific points made in the individual filing of Dr. Philip Stark;
- clearly underscore that, to be as secure and verifiable as possible, *all* voting technology must be: ***isolatable*** from inherently vulnerable networks of all kinds; ***inspectable*** with very high confidence at every stage of operation; and ***interoperable*** to maximize efficiency and system modernity.

The Committee thus specifically and emphatically recommends that the final VVSG:

1. **Endorse a blanket ban on the internet connection capability of any and every voting technology addressed by the VVSG, *including connection to any private network that ultimately may connect to the internet*.** This categorical prohibition on the inclusion of any connectivity-enabling devices in election-related equipment include all wireless modems, radios, and any other type of equipment capable of communicating over the internet. *Simply disabling such devices if installed will not suffice to protect election networks, databases and equipment.*
2. **Foster and justify public confidence that our election results are wholly evidence-based by requiring that elections be fully and robustly auditable.** To accomplish this goal, *all post-election ballot audits must occur before results are finalized and certified.* Moreover, such universal post-election assessment must include both *compliance audits* that verify the audit trail and *risk-limiting* ballot audits that either validate the declared results or determine what the correct results should be.
3. **Require the full interoperability of all internal voting system components, peripherals and data formats, together with component and system integration testing and certification.** Component testing would significantly decrease vendor development and testing costs. Component certification, combined with interoperability, almost certainly would decrease the costs and increase the options of election officials by facilitating the modular replacement of only those portions of their systems that require upgrading rather than systems in their entirety, as is now the norm. Component testing also would lower the barriers to market entry for new and potentially innovative component-producing companies which would be relieved from the present burdens of having to develop complete election systems.

² The Committee has carefully reviewed and emphasizes in the attached Appendix select observations and recommendations of the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), and Verified Voting (VV).

Thank you again for the opportunity to participate in this critical effort. Should you or your staff have any questions regarding these Comments, or seek further expert analysis or information our members may provide, please email Adam Eisgrau, ACM's Washington-based Director of Global Policy & Public Affairs, at the address below or reach him at 202-580-6555.

Sincerely,



James A. Hendlar, Chair

Appendix

Appendix

ASSOCIATION FOR COMPUTING MACHINERY U.S. TECHNOLOGY POLICY COMMITTEE COMMENTS ON EAC VVSG 2.0 ADDITIONAL CONCEPTS AND COMMENTS ENDORSED

ACM's U.S. Technology Policy Committee also makes the following additional general points (unattributed) and associates itself with the specific analyses of VVSG 2.0 identified below articulated variously in their Comments by: the Electronic Privacy Information Center (EPIC), National Election Defense Coalition (NEDC), State Audit Working Group (SAWG), Verified Voting (VV), and Dr. Philip Stark (PS).

Principle	Issue	Comment/Analysis	Source(s)
General	Structure	<ul style="list-style-type: none">▪ Separation of proposed principles from detailed technical requirements.	PS
General	Process	<ul style="list-style-type: none">▪ Approval of technical requirements and test assertions without EAC vote.	VV
General	Objective	<ul style="list-style-type: none">▪ VVSG must: "deliver meaningful and effective guidance and requirements that will improve the security of voting systems and lessen exposure to manipulation, tampering or hacking."	NEDC
General	Auditability	<ul style="list-style-type: none">▪ Our nation must conduct and verify fully auditable evidence-based elections.	PS, SAWG, VV
General	Connectivity	<ul style="list-style-type: none">▪ No device involved in balloting or election administration should be connected <i>or connectable</i> to the internet or any private network that connects to the internet.	EPIC, NEDC, PS
4	Interoperability	<ul style="list-style-type: none">▪ Strongly supported for all devices and data.	
5	Voter Access	<ul style="list-style-type: none">▪ Voters must have equal and consistent access to election systems and resources.	
6	Voter Privacy	<ul style="list-style-type: none">▪ Voter privacy must be assured and protected in all phases of the election process.	
7	Balloting	<ul style="list-style-type: none">▪ Ballot text, form and vote selections must be presented in a clear and understandable way that can easily be marked and verified by all voters.▪ Voting systems must allow voters to consistently and accurately verify both their ballots and the auditable records of their votes.▪ Voters with disabilities must be able to independently validate their ballots.	VV PS

8	Voting Systems/ Processes	<ul style="list-style-type: none"> ▪ Voting systems and processes must be “robust, safe, usable and accessible. ▪ 8.3: System accuracy and ease of use must be prioritized over voter “satisfaction.” 	PS
9	Auditability	<ul style="list-style-type: none"> ▪ 9.2: Election/voting records must be verifiable by the voter. 	VV
10	Ballot Secrecy	<ul style="list-style-type: none"> ▪ It should not be possible to link the voter to his or her ballot once the ballot has been cast. ▪ “Voters should vote privately . . . but votes should [more accurately] be [considered and described as] anonymous rather than secret.” ▪ Delete “recallable ballot” from the glossary as the notion of a recallable ballot inherently conflicts with a ballot secret and anonymity. 	EPIC PS SAWG
13	Data Protection	<ul style="list-style-type: none"> ▪ Add a separate guideline articulating the clear prohibition on internet “connectivity,” above. 	NEDC
15	Detection and Monitoring	<ul style="list-style-type: none"> ▪ 15.4: As this provision presumes the interconnection of voting systems with the internet or other networks in contravention of the recommended prohibition, it should be eliminated. 	PS
Glossary		<p>The Committee also concurs that the following key Glossary terms should be added or modified:</p> <ul style="list-style-type: none"> ▪ Audit ▪ Ballot ▪ Ballot Secrecy ▪ Ballot Selections ▪ Cast Vote Record ▪ Correct (re: election outcomes) ▪ Effectiveness ▪ Efficiency ▪ Resilience ▪ Sensitive Data ▪ Voter Selections 	PS PS, VV SAWG, VV SAWG PS, SAWG, VV VV PS PS SAWG VV SAWG



Testimony of

Joseph Lorenzo Hall, PhD

Chief Technologist

The Center for Democracy & Technology¹

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 29147/30111⁶). 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-e slate-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 collaborators⁸ 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 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/>.



DISABILITIES LAW PROGRAM

COMMUNITY LEGAL AID SOCIETY, INC.

100 W. 10th Street, Suite 801
Wilmington, Delaware 19801
(302) 575-0660 TTY (302) 575-0696 Fax (302) 575-0840
www.declasi.org

May 29, 2019

VIA ELECTRONIC SUBMISSION

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Public Comments on Voluntary Voting System Guidelines (VVSG) 2.0 Principles and Guidelines

The Disabilities Law Program of Community Legal Aid Society (“DLP”) appreciates the opportunity to comment on the draft Voluntary Voting System Guidelines 2.0. Principles and Guidelines. The DLP is the designated Protection and Advocacy (P&A) system for individuals with disabilities in Delaware. Through the Protection and Advocacy for Voter Access (PAVA) program, created by the Help America Vote Act, the DLP has a federal mandate to “ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote and accessing polling places.”

DLP applauds the US Election Assistance Commission (EAC) for attempting the complex task of balancing election security with federal elections accessibility requirements under law. Yet, DLP remains concerned that the only voting systems capable of meeting VVSG 2.0’s requirements will be reliant on a marked paper ballot as the ballot of record, a concern that has been further confirmed by the technical standards for the VVSG that are currently being developed in public forums. It must be acknowledged that the promise of fully accessible, paper-based voting systems is as old as the passage of HAVA itself. Yet, the dream that paper ballots will be made accessible, private and able to be cast independently, for people with disabilities is not now, and may never be, a reality. Widespread implementation of market-ready, fully accessible paper ballot voting systems is simply not achievable within the foreseeable future.

Further, VVSG 2.0 adheres to the misguided concept of “one accessible system per polling place.” The assumption that voting accessibility is limited to use of a ballot marking system at a traditional polling place neglects the rapidly expanding opportunities to participate in the electoral process outside a visit to one’s neighborhood polling place. Increasingly, voters with disabilities and their non-disabled peers are leveraging opportunities to vote by mail, vote absentee, and may be receiving their ballots electronically. Yet, VVSG 2.0 denies these voters the guarantee of an accessible ballot by limiting the extent of the VVSG’s reach into non-traditional voting systems.

The DLP believes that the failure of VVSG 2.0 to apply its accessibility guidelines beyond one voter station per polling place will enable segregated systems of voting. Segregated electoral

KENT COUNTY
SUSSEX COUNTY

840 Walker Road, Dover, DE
20151 Office Circle, Georgetown, DE

(302) 674-8500
(302) 856-0038

DELAWARE'S PROTECTION AND ADVOCACY SYSTEM FOR PERSONS WITH DISABILITIES

processes restrict any voter that benefits from use of the accessible voting system to a separate line, while more able-bodied voters hand mark their paper ballots. Segregated systems are a form of discrimination and inherently unequal and should no longer be considered a standard, acceptable practice in the United States.

In practice, segregated voting practices are already known to be riddled with problems for voters with disabilities. The assumption that a majority of voters will hand mark their ballots means that there are a limited number of accessible voting machines present. Poll workers are insufficiently prepared to operate them. As a result, poll workers at their best are unable to describe and activate accessibility features included in the equipment's design. At worst, elections personnel discourage use of the equipment by voters or leave the voting machine turned off, still in its case, and even hidden from view. For the few voters that are able to cast their ballots on the one accessible system available, the secrecy of their ballots cannot be guaranteed. The ballots inevitably vary in appearance from hand marked ballots and may even be tallied and stored separately.

While DLP believes that America's elections must be accurate and understands the desire to address the concerns of cybersecurity advocates, the VVSG is widely used by voting technology manufacturers to guide the development of their products and by state and local elections officials to inform purchase and implementation of voting equipment. Consequently, it behooves the EAC, in this process of a comprehensive re-envisioning of the guidelines, to expand the VVSG's reach to encompass all technology used to cast ballots within or beyond the traditional polling place. *Further, and most importantly, the VVSG must ensure a private and independent ballot for all voters in a fully integrated experience that respects the dignity of the voter and the secrecy of the ballot.*

Sincerely,



Laura J. Waterland, Project Director
Disabilities Law Program
lwaterland@declassi.org

AUDIT USA

Americans United for Democracy, Integrity and Transparency in Elections

Letter to EAC on May 29th, 2019.

To whom it may concern:

AUDIT Elections USA focus is based on making the black box into a transparent box, ensuring that the results match and accurately represent the will of the voters.

We are a nonpartisan organization whose mission for the last 15 years is to restore public ownership and oversight of elections, to work to ensure the fundamental right of every American citizen to vote and to have each vote counted as intended in a secure, transparent, impartial, and independently audited election process.

We at AUDIT Elections USA are finding that many states have switched from the optical scanners to digital scanners. By the 2020 presidential election, about 75% of all hand-marked paper ballots are now counted by digital scanners that produce a public record called ballot images which are an exact copy front and back of the ballot. That good news!

However, many jurisdictions that have digital scanners claim that they are preserving the ballot images when in reality they are only preserving the write-in ballot images only.

As to the illegal destruction of ballot images, expert witness Dr. Thomas W. Ryan, who holds a Ph.D. in Electrical Engineering and has over 30-years' experience in digital image creation, processing and interpretation, said in his affidavit in our Arizona ballot images case: "In Summary, deleting ballot images significantly undermines the integrity of the election system that derives all its tabulation data from those images."

In a Pima County lawsuit, the judge properly recognized that images were part of the chain-of-custody when he stated and clearly ruled that they are a public record. <http://bit.ly/2WtINEj>

Tucson AZ, Superior Court Judge Gordon asked the attorney for Pima County, "If you take voted ballots, make a copy of them and use those copies to count votes, what makes you think that you can destroy them?" Link to Pima video 2nd Court Hearing Oct 14, 2016, at 9:30 minutes. <http://bit.ly/2I8GtJE>

THE IMPORTANCE OF BALLOT IMAGES: First off, they are those who claim that Hand Marked Paper Ballot's IMAGES could be hacked. We say at AUDIT USA that the original Hand Marked Paper Ballot could be hacked too! We know that hand-marked paper ballots could be manipulated if the chain of custody is not secure, and there are those who are concerned that ballot images could be hacked. However, here's the beauty of ballot images – it's REDUNDANCY! It is the redundancy of having BOTH the hand-marked paper ballots AND the ballot images that TOGETHER create a unique, end-to-end verification of the election. The ballot images, if posted immediately and publicly, memorialize the hand-marked paper ballots so they cannot be switched out for a recount or an audit.

In other words, the ballot images are part of the chain of custody and prevent manipulation of the paper ballots. A risk-limiting audit can be done to ensure that the ballot images correctly reflect the paper-ballot votes.

The fact is that the ballots and the ballot images protect each other, adding a layer of protection against hacking.

AUDIT USA

Americans United for Democracy, Integrity and Transparency in Elections

My Arizona attorney and best friend Bill Risner says they are destroying the ballot images in most states because they're protecting the right to cheat now or in some future election. They like the old system of the black box that left no evidence behind.

We see these ballot images as impunity busters. Many jurisdictions are destroying them, which is illegal because the images become public records the millisecond they are made.

I can assure you as a fact, that a digital image scanner does not work at all unless it first creates a digital ballot image. Indeed, even the promotional material of ES&S, the largest vendor that provides digital image scanners, states that the images are to be used for "auditing and adjudication" of election results, by utilizing ballot images.

Furthermore, nationally AUDIT USA and many other election activists are seeing a dangerous trend which seems to be a repeat of previously failed voting infrastructure and concepts. This current push by election equipment vendors to sell a device called a Ballot Marking Device, or BMD, that has already been proven to be very expensive and potentially of some danger is very concerning.

A BMD is basically a Direct Recording Electronic, DRE touchscreen voting machine that has an electronic ballot that is computer-generated instead of being hand marked by a voter. They claim that it produces a ballot when it creates what we call a Cast Vote Record. A ballot has choices, while a Cast Vote Record is merely a record of the votes produced and marked by a machine. Additionally, this introduces another unnecessary, insecure, and error-prone computer system to the already murky mix.

If a recount was to happen, machine printed ballots are far easier to counterfeit than paper ballots, uniquely hand-marked by a human are much harder to counterfeit.

Moreover, along with these DRE / BMD marking devices, they want you to trust a BAR CODE to be used to transmit your vote as part of the chain of custody. These Bar Codes can also be gamed, and they're not readable by a human eye, bringing into question transparency and accountability issues.

Another process that bothered us about elections is how elections are certified. On election night they say that the results are unofficial, giving the appearance that there will be procedures like audits to check for accuracy and completeness before they certify the election. I find certification is NOT derived from doing random audits or even accounting style review. It's no more than a deadline of a specified day that they are given to turn in results. They get together on that date and submit the results they have at that point from the central tabulator without further verification. What a system! This is how it's done around the country in most places.

The only state that I know of at this time that is actually filing a certified election report based on a 100% audit is the state of Maryland. They do a complete independent audit utilizing all the ballot images. Moreover, they do find problems, and it is all transparent.

Maryland's transparency policies have helped candidates decide whether to go for a recount or not. Moreover, that saves a lot of time and money. Besides, it's a one hundred percent transparent solution.

Here is a link to Steven Rosenfield's incredible coverage below on the subject of verified elections. "Does Maryland have the answer for verifying America's vote count?"

AUDIT USA

Americans United for Democracy, Integrity and Transparency in Elections

Also, While in Broward County, Florida, for the November election, I filmed and provided several videos showing proof of the use of cellular phone modems to the non-profit news organization, WhoWhatWhy, "NEW VIDEO PROVIDES PROOF OF CELLULAR MODEMS IN FL VOTING MACHINES."

Cellular modem transmissions are encrypted, and the modems are internet connected. As I said before, we are not worried about outsiders, it's an insider's game, and with cellular modems, they don't even have to be in the building.

Well know DC Attorney Chris Sautter, and I first found the modems in the 2016 Wisconsin presidential recount in Milwaukee.

For the most part, counties in Wisconsin that refused to hand count were the counties with the built-in cellular phone modems which are connected to the internet. I was surprised when we found them because of this report on Sep 30, 2016, in the Chicago Tribune where the "FBI Director James Comey told lawmakers that the agency is looking "very, very hard" at Russian hackers who may try to disrupt the U.S. election. ... and then Comey ensured lawmakers that the electronic voting machines are not connected to the internet."

Well, that was not what we found in Wisconsin.

This is crazy stuff. They are focused on the threat of outsider hacking when statistically most fraud is done by insiders...and they never talk about it, and that's very wrong!

The election department and vendors have many insiders, employees, temporary employees and ex-employees which some of them, are now high paid consultants running elections all over the country, and some are controlling these elections remotely.

Many folks might be shocked by what we found, but I'm not! We found the same kind of things going on in Wisconsin, Rhode Island, Florida, and the destruction of ballot images in Arizona, Alabama, Ohio, Virginia, North Carolina, and other states. Particularly in the largest counties of people of color in Alabama, Ohio, and Florida.

Our final request, please protect our secret ballot. There should be no unique identifiers on a ballot identifying voters. At this time, I'm in North Carolina investigating and have found that all early ballots cast have a unique identifier on them. They say that's on there in case somebody was to vote twice or die before election day.

Nonsense. Voting is a secret process; counting is a public process. We understand that Texas and North Carolina are insisting that they have the right to do this. Outlaw this and protect our vote.

Respectfully,

John R Brakey

Director and Co-founder; Americans United for Democracy Integrity and Transparency - AUDIT-ELECTIONS-USA

JohnBrakey@gmail.com

<http://www.auditelectionsusa.org/>

<https://www.facebook.com/AUDIT.USA/>

<https://www.facebook.com/john.r.brakey>



May 28, 2019

U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Re: Public Comment on VVSG 2.0 Principles and Guidelines

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

Microsoft Corporation is writing to express our strong support for the VVSG 2.0 Principles and Guidelines document, which we feel is an important step towards improving election technology security in the United States. In addition, we would like to make recommendations for small but important edits to guidelines within principles 10 and 13. Finally, we hope to highlight ongoing work Microsoft is conducting relevant to election technology security. Microsoft's comments are based on its longstanding commitment to support stronger election security, and the company is not involved in the commercial sales of election systems or software.

Microsoft strongly supports the VVSG 2.0 Principles and Guidelines, including both the language of the Principles and Guidelines as written in general, as well as the development process of the Principles and Guidelines. Microsoft applauds the Election Assistance Commission's work on establishing the Principles and Guidelines and urges the Commission to vote to approve the document.

Microsoft specifically emphasizes the importance of Principle 9: Auditability and the supporting Guidelines 9.1 through 9.4. These guidelines are crucial to maintaining election integrity and are well-reasoned and achievable. Guideline 9.1 implements the critical property of software independence, which ensures that faults in election systems are detectable. Guidelines 9.2 and 9.3 ensure that election data that enables proper auditing is provided and preserved. Guideline 9.4 explicitly ensures that proper auditing is supported by compliant election systems. Together, these guidelines are important and reasonable measures to enable auditors to verify the accuracy and integrity of election outcomes.

Microsoft sees slight technical problems with guideline 10.2, within Principle 10: Ballot Secrecy. As worded, the guideline can be read to disallow provisional ballots. The guideline may also be read to prohibit the publication of encrypted ballot contents, even when decryption requires explicit cooperation of a majority of canvassing board members and when this publication can enable greater transparency and verifiability, in addition to providing better privacy for provisional voters. We suggest the following wording clarification. **"The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections without an appropriate administrative process."**

Microsoft additionally sees an important technical problem with Guideline 13.3, within Principle 13: Data Protection. As worded, the guideline could be read to prohibit end to end (E2E) verifiable systems. E2E verifiable systems use homomorphic encryption to provide greater transparency, integrity



and verifiability to elections. However, homomorphic encryption methods are not well-standardized. In particular, the ElGamal encryption system – while well-recognized and accepted in the cryptographic community – has not been subjected to a traditional standards process'. It is effectively nothing more than a standard Diffie-Hellman key exchange followed by use of the exchanged key as a one-time pad and thus should not be excluded from use in an accepted and trusted voting system. We suggest the following wording clarification. "All cryptographic algorithms are public, well-vetted, and – where applicable – standardized."

On May 6th, Microsoft announced the upcoming release of ElectionGuard, a free open-source software development kit designed to make voting secure, more accessible and more efficient. ElectionGuard, developed with the assistance of our partner Galois, will be made available this summer to election officials and election technology suppliers who can incorporate the technology into voting systems. ElectionGuard will enable E2E verification of elections, open results to third-party organizations for secure validation, and allow individual voters to confirm their votes were correctly counted. Microsoft has partnered with several major election technology suppliers to explore the integration of ElectionGuard into voting systems. ElectionGuard is designed to supplement, not replace, current and future voting systems.

Microsoft thanks the Commission for its consideration and looks forward to continued engagement on this important issue.

Sincerely,

A handwritten signature in black ink that appears to read "Tom Burt".

Tom Burt
Corporate Vice President, Customer Security & Trust
Microsoft Corporation



NATIONAL ASSOCIATION of STATE ELECTION DIRECTORS

Thank you for the chance to provide feedback on Version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0). The VVSG 2.0 represents an important opportunity to advance modern voting system standards that election vendors can use to build secure, trustworthy voting technology that voters can have confidence in.

The National Association of State Election Directors (NASED) represents all 50 states, the District of Columbia, and the five U.S. territories: American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands. Our members serve on the Technical Guidelines Development Committee (TGDC), the Election Assistance Commission's (EAC) Board of Advisors, and the EAC Standards Board; NASED itself had a VVSG Committee when there was no quorum at the EAC to discuss solutions for moving the standards development process forward without the EAC.

The EAC has asked for feedback from the community on both the content of the VVSG 2.0 and the proposed structure. VVSG 1.0 was approved by the EAC in December 2005; in 2007, an effort to make significant changes to the VVSG and move to version 2.0 failed because the commissioners could not agree. In 2015, the commissioners approved minor modifications to version 1.0, updating the standard to version 1.1¹. To put this in perspective, Apple released the first iPhone in June 2007; the current voting system standards are so technologically dated, they predate the first iPhone because the EAC commissioners could not agree on more significant revisions.

Standards must fit the world that we live in, and this requires the ability to change and adapt quickly. The proposed structure makes the Principles and Guidelines the VVSG 2.0 and leaves the technical requirements and voting system test lab test assertions separate, and therefore not in need of a vote by EAC commissioners; these additional documents would be updated consistent with a policy which would be voted on by EAC commissioners. The TGDC, the EAC Standards Board, and the EAC Board of Advisors, all of which include diverse state and local election officials and non-voting representatives from the EAC itself, voted in favor of the proposed

¹ In software development, major changes result in a change to the first digit and minor changes result in a change to the second digit; thus VVSG v.1.1 represents minor changes to VVSG v. 1.0.

structure of the VVSG 2.0 in September 2017 and April 2018, respectively. Both the TGDC and the Board of Advisors also include technology and accessibility experts in addition to state and local election officials.

At the 2018 EAC Standards Board meeting, however, the EAC offered that EAC commissioners should not only vote on the Principles and Guidelines but on the requirements and the voting system test lab test assertions as well. This was a surprise, and defeats the purpose of designing the VVSG 2.0 as a separate document from the requirements and test assertions. Based on questioning at the Public Hearings on the VVSG 2.0 on April 10 and April 23, 2019, it is clear that the EAC commissioners continue to think this is the appropriate course of action; NASED disagrees. EAC commissioners have never cast a vote on voting system test lab test assertions.

NASED strongly supports the proposed structure of the VVSG 2.0 out for public comment, with the broad, high-level Principles and Guidelines requiring EAC commissioner approval and allowing the technical requirements and voting system test lab test assertions to be updated regularly by qualified EAC technical staff in close consultation with other experts, including those from the National Institute of Standards and Technology (NIST). This proposed structure will allow the testing and certification processes to be more efficient and permit new methods for certifying modifications, upgrades, and patches, all of which will allow election officials to better ensure the security and integrity of their voting equipment.

Consistent with the recent unanimous recommendation of the EAC Standards Board and the resolution passed by the EAC Board of Advisors, NASED views the Principles and Guidelines as the VVSG 2.0, required by the Help America Vote Act of 2002 (HAVA) and subject to EAC commissioner vote. Prior to adopting the VVSG 2.0, however, the EAC must also adopt policies governing the VVSG 2.0 that clearly state that the requirements and voting system test assertions are independent documents that do not require commissioner vote. This will allow the requirements and test assertions to be dynamic over time, even when there is no quorum of commissioners at the EAC.

EAC commissioners voting on requirements and test assertions is problematic for several reasons:

- The EAC is often without a quorum. If the requirements and test assertions are considered part of the VVSG 2.0, they cannot be updated in the absence of a quorum.

NASED's concerns about a quorum at the EAC are not unjustified; in fact, the agency was without a quorum almost as soon as it was voted into existence. The EAC should have had a quorum within 120 days of the date of HAVA's enactment, or by February 23, 2003; the initial commissioners, however, were not appointed until December 13, 2003.² The EAC had a quorum from that date until December 10, 2010³, when Commissioner Gracia Hillman left the agency. The EAC went without a quorum again until January 13, 2015,⁴ and for another 317 days in 2018 and 2019 during which time Microsoft alone issued a dozen critical patches for its products.⁵ In total, the EAC has been without a quorum for 2,105 days⁶, or 35.6 percent of the agency's entire existence.

- The structure of the EAC – two Republican-appointed commissioners and two Democratic-appointed commissioners – makes the agency susceptible to politics. Voting system standards are not political or partisan, and cannot be hamstrung by a deadlock among the commissioners, particularly given that the commissioners typically are not technical experts. The development of the VVSG 2.0 has been a bipartisan, collaborative process from the very start, and the TGDC, Standards Board, and Board of Advisors are all bipartisan.

² [Testimony of the EAC Commissioners](#) before the U.S. House of Representatives Committee on House Administration, June 17, 2004. See page 1.

³ [Amended Notice: Request for Substantive Comments on the EAC's Proposed Requirements for Version 1.1 of the Voluntary Voting System Guidelines \(VVSG\)](#), published in the Federal Register October 1, 2012.

⁴ [EAC Major Management and Performance Challenges report](#), submitted to EAC Acting Executive Director Alice Miller by EAC Acting Deputy Inspector General Roger LaRouche, October 13, 2015. See page 3.

⁵ Data on critical patches courtesy of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).

⁶ February 23, 2003 to December 13, 2003 is 293 days; December 10, 2010 to January 13, 2015 is 1,495 days; March 24, 2018 to February 4, 2019 is 317 days. As of May 2, 2019, the EAC has been in existence for 5,912 days.

- Technical standards must be reviewed and approved by technical experts, not political appointees. At the EAC, the appropriate approver for technical standards is the Director and staff in the Testing and Certification department of the agency, in consultation with NIST and others, similar to how the EAC Executive Director and Director of Testing and Certification are responsible for the certification of voting systems. The commissioners must trust their staff and technical experts.
- The EAC commissioners have never voted on voting system test lab test assertions. The commissioners should not vote on more than they already do: VVSG 1.0 predates the iPhone because the commissioners could not agree on more significant changes to the standards.

Test assertions represent the process by which the test labs will achieve the requirements, and therefore they must be modified on an ongoing basis to make sure that they continue to adequately test the requirements. The EAC did not vote on the current test assertions and has never voted on them in the past; some of the current test assertions were developed by the EAC and NIST and the rest are, according to EAC staff at the 2018 Standards Board meeting, “proprietary to each of the labs.”⁷ While we appreciate efforts to standardize the test assertions across voting system test labs, NASED does not believe that it is appropriate for non-technical experts to vote on highly technical procedures. The test assertions should be maintained via a public process and reviewed and approved by EAC technical staff in consultation with NIST.

The proposed VVSG has been formally in development since 2015, though NASED members began discussing this proposed structure as early as 2013 on the NASED VVSG Committee. Over the last four years, technology and accessibility experts, voting system vendors, and federal experts, including representatives from NIST and the EAC itself, have contributed to the Principles and Guidelines as well as to the development of the requirements and test assertions. TGDC meetings are public, and the working groups focused on the requirements’ development, also public, include dozens of current and former state and local election officials from jurisdictions across the country, as well as voting system vendors, advocates, and others. The time to raise concerns about taking the requirements out of the VVSG was when the new structure was first proposed. Now that we are so close to the finish line, and now that the security threats we face demand it more than ever, we cannot begin the standards development process again from scratch.

⁷ [Transcript of the 2018 EAC Standards Board Meeting](#), April 19-20, 2018 in Coral Gables, Florida. See pages 208 and 223.

State and local election officials, not the EAC or EAC commissioners, bear the brunt of public ire and media hostility when voting systems are out-of-date; the election administration community needs the VVSG 2.0 to pass in the proposed flexible form. The Principles and Guidelines independent from the requirements and test assertions are what the election administration community wants, and more importantly, what it needs to meet modern security standards and maintain voter confidence in our election process. It is critical that there be a mechanism for updating the technical requirements and test assertions for voting systems that does not require EAC commissioner approval. The integrity of American voting systems cannot be held hostage by lack of a quorum or philosophical differences among the commissioners. There is too much at stake.

Keith Ingram, President, NASED

Lori Augino, Incoming President, NASED

Michelle Tassinari, Vice President, NASED

Steve Trout, Treasurer, NASED

Sally Williams, Secretary, NASED

Rob Rock, Northeast Regional Representative, NASED

Jared Dearing, South Regional Representative, NASED

Meagan Wolfe, Midwest Regional Representative, NASED

Wayne Thorley, West Regional Representative, NASED

Robert F. Giles, Immediate Past President, NASED

Judd Choate, NASED

Linda Lamone, NASED

May 27, 2019

U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

To the members of the U.S. Election Assistance Commission,

I appreciate the opportunity to comment on revisions the Federal Voting System Guidelines.

I am very concerned about the ES&S ballot-marking computers that the state of Georgia is considering purchasing. Officials have not made public their final decision, but it appears that the ES&S ExpressVote system is most favored. Dominion ImageCast is also being considered. Both models embed voter selections in problematic barcodes (ES&S) and QR codes (Dominion).

Voters cannot read barcodes or QR codes, so when their votes are embedded in codes, voters have no idea if what they intended to cast was accurately recorded. When those same barcodes or QR codes are tabulated—not human readable marks—the voter has absolutely no reassurance that their votes were counted as cast. If audits are attempted, they are meaningless because the data on which they are being audited is questionable.

Voter chain of custody of the vote is a bedrock requirement in democratic elections. Ballot marking computers that embed votes in barcodes or QR codes remove any notion whatsoever that voters are in charge.

The nation's top IT experts agree that security is compromised with all voting computers. Hand marking on paper is the most secure method to record votes. There is nothing to come between the voter and his recorded vote, and that authentic ballot becomes the ballot of record for audits.

Reviewing the Voluntary Voting System Guidelines 2.0, I see serious inconsistencies between what is stated in the Principles and Guidelines and the realities of ballot marking devices.

1.2 Ballot marking devices are not tested in election mode, only in test mode, hence, not “real-world operating conditions.”

2.2 “User-centered design methods” cannot include embedding voters’ choices in barcodes or QR codes. Users have no idea if their votes are being recorded and tabulated correctly. User loses chain of custody of the vote.

2.3 Voting system logic is not “clear and meaningful” if votes are hidden from voters in barcodes or QR codes at any point in the voting process.

2.5 Data has no integrity if it is acquired while obscuring any part of the chain of custody of the vote. Barcodes and QR codes hide the vote, so voters have lost a significant part of the chain of custody of the vote, and can no longer trust the data that is acquired.

2.6 There is no evidence that current models of ballot marking devices have sufficient provisions for handling errors in a robust manner. Poll workers would need more extensive training than they currently receive to be able to handle many failures.

3.2 As these are proprietary systems, the public has little or no access to inspect processes and transactions, especially if the Secretary of State is not open and transparent to his public.

3.3 This is the most crucial point—the public cannot understand or verify the operations of the voting system if their votes are lost in barcodes or QR codes. The voter's chain of custody of the vote is completely compromised.

5.1 Ballot marking devices have a totally different format and interface from absentee and provisional ballots, making the voting experience inconsistent. Voters deserve at least a full face ballot, not the contrived "scanning ballot" of the ES&S ballot marking device.

7.3 There is no guarantee that voters can understand all information, especially error messages. The system is complicated and that level of knowledge of computer technology is beyond the understanding of many poll workers to assist voters.

9.1 Absolutely an error or fault can cause an **undetectable change** in election results, especially with the "all-in-one" models. It is a closed system.

9.2 The records that are provided are flawed because they produce information that cannot be authentically verified by voters. Does the list on a "scanning ballot" actually match the information embedded in the barcodes? "Scanning ballots" are in a format that makes verifying them very difficult for the average voter, and research shows that most people do not take the time to check their votes in the list, so they could easily not notice any divergence from what they cast. Voters should not be tasked with verifying the accuracy of a computer.

9.4 Data from "scanning ballots" cannot be used for any kind of audit, because it was obtained without transparency, hidden in barcodes or QR codes. Voters cannot trust the data that are tabulated or used for audits.

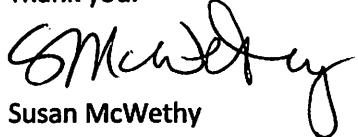
12.1 Currently the mechanisms used in the state of Georgia to protect and detect unauthorized physical access to DRE computers are not secure. They consist of plastic cable ties that can easily be cut through or opened without detection.

13.2 The source and integrity of tabulation reports are not verifiable because of the barcodes and QR codes that produce questionable data.

15.4 IT experts agree that no defense exists against network-based attacks.

I hope you will take seriously the many complications and problems with ballot marking devices, especially those that embed voter selections in barcodes and QR codes. They are not secure, and they have the potential to create undetectable outcomes that defy the integrity of the voting process.

Thank you.



Susan McWethy
Decatur, GA
404-354-6178

To the Election Assistance Commission:

I welcome the new VVSG 2.0 as a significant improvement to the current voting system guidelines. However as drafted, the VVSG 2.0 provides inadequate security and will not be able to assure voters that their votes are being counted as cast. Additionally, the drafting process has been flawed because it is too reliant on the biased input of voting system vendors, who have not historically shown a commitment to election security.

I ask that you make sure that all systems approved by the VVSG 2.0 meet the following standards:

NO APPROVED VOTING SYSTEM WILL :

1. ... record votes directly to a computer memory without the voter reviewing a paper ballot.
2. ... have a modem or allow remote access.
3. ... allow the technical opportunity for a machine to change a ballot after the voter has cast it – even if the machine is under the control of malware.
4. ... be a hybrid machine – with a printer and a scanner in the same path.
5. ... encode votes using barcodes, QR codes, or any other format that is not verifiable by a voter without assistive technology.
6. ... allow weighted election functions that use decimal counting methods. Votes must be counted as whole numbers.

ALL APPROVED VOTING SYSTEMS WILL

7. ... allow for the use of hand-marked paper ballots - not just a paper trail created by a machine, except for accommodations made for voters with disabilities.
8. ... use durable paper, not thermal paper.
9. ... support the ability to have an accurate hand-counted audit.
- 10.... create a digital ballot image that is identical to the paper ballot.

- The EAC must create a panel of election security experts made of academics and technical experts with no relationship to vendors and no vested interest in emerging systems. The EAC needs to take input on the VVSG 2.0 from this panel - and other non-vested security experts on an ongoing basis.
- The EAC must stop consulting vendors and their representatives for technical guidance. This is a conflict of interest, is unethical and is preventing security improvements from being implemented.

Sincerely,
Aimee McCullough

Jack Cobb, Pro V&V Laboratory
EAC Public Meeting
May 19, 2019

Thank you, Madam Chair and Commissioners.

I am honored to have this opportunity to be here today. Thank you for extending me the invitation to come and discuss this important topic.

I would like to begin by stating I have participated in many panels and testified in a few public hearings, but this is the first time I believe I have been in the presents of a full Commission of United States Election Assistance Commission. It is good to see and I hope it remains this way.

Some five years ago, stakeholders in this industry were in a much different place. At this time, this commission did not have a single Commissioner, much less a quorum. There had not been a Commissioner since December of 2011. The standard last adopted by the EAC Commission was the 2005 EAC VVSG. NIST had written the “Next Iteration” or the 2007 VVSG and completed updating the VVSG 1.1, but nothing could be done with these standards because the 2002 Help American Vote Act or HAVA states the following:

(1) IN GENERAL.—A voluntary voting system guideline described in subsection (b) (or modification of such a guideline) shall not be considered to be finally adopted by the Commission unless the Commission votes to approve the final adoption of the guideline (or modification), taking into consideration the comments and recommendations submitted by the Board of Advisors and the Standards Board under subsection (c)

I don't believe when HAVA was adopted that Congress thought there would ever be a time when there were no Commissioners. Well that did occur, and the amount of time this went on for was measured in years not months. Updating the standards was not a slow process or that adoption was taking too long, it was simply we had to work with standards that were set in time and could not be updated without a quorum of the Commission.

With this reality, stakeholders started to really look at making the process of adopting, modifying, and testing to the standards more agile. Also, meetings were being held and discussion were had not only about the process, but also about the content. The main question about the Standard was "Do we want a design standard or a high-level guide that allowed for technology to solve problems as it advanced. These meetings and discussions went on for about year and it was determined that in order to develop voting system as modern as technology allows, we should move to a more high-level group of principles that do not take current technology into account.

The new VVSG 2.0 we are discussing here today was developed to be a standard that once adopted would stand for a long period of time without the need for modification because of technology changes, or security postures changing. This standard is laid out with 15 major principles that a voting system must meet to ensure the reliability and integrity of American Elections.

Again, I thank you Madam Chair and Commissioners for allowing me the opportunity to speak to you on this important topic. I will be happy to answer any of your questions.

VVSG 2.0 Principles and Guidelines – Public Hearing

May 20, 2019

Good afternoon Chairwoman McCormick, Commissioner Hovland, Commissioner Palmer and Commissioner Hicks. I'd like to thank all of you for having me here today. My name is Traci Mapps. I'm the Director of SLI Compliance. I have been with SLI for over 11 years overseeing our Voting System Test Lab and I have worked in the software test industry for over 20 years.

As you know, SLI is one of two accredited Voting System Test Labs under the EAC and NIST/NVLAP. We are also an Authorized Test Lab and an Authorized Certification Body by the U.S. Department of Health & Human Services, Office of the National Coordinator providing test and certification services for meaningful use and accredited by both NIST/NVLAP and ANSI.

SLI has been an Independent Test Authority for voting system certification testing since the National Association of State Election Directors first established a certification program in 2001 for voting system certification. We employ a long-tenured and experienced team of credentialed voting system test and security professionals and we have experience with nearly every voting system being used in the U.S. today. To date, we have been authorized to conduct certification testing across all VSS and VVSG standards and we have completed a number of EAC test certification engagements across all of these standards, with the exception of VVSG 1.1 which no voting system has been tested to under the EAC test and certification program as of yet. Not only does SLI perform federal certification testing under the EAC, but we also provide security and certification testing services directly to several states including but not limited to California, New York, Pennsylvania and Virginia. SLI also participates in the Department of Homeland Security's Sector Coordinating Council (SCC) for the Election Infrastructure Subsector.

Federal certification testing includes testing of all the existing 1000 plus requirements that include functional testing, usability and accessibility, hardware testing, software analysis, telecommunications testing, security testing, quality assurance and configuration management audits and more. Based on this, I feel

that SLI, and Pro V&V, have an unmatched expertise when it comes to the voting system standards and the understanding of testing systems to these standards for certification.

With the two public hearings that have already taken place before this one, you've already received much input and feedback from the election community. I appreciate you inviting me here today to provide a statement in regard to the proposed VVSG 2.0 Principles and Guidelines from a Voting System Test Lab standpoint. Since SLI has not seen any of the requirements or test assertions that have been developed for VVSG 2.0, I'll provide you with my thoughts on the proposed Principles and Guidelines at this time.

As we all know and we have heard throughout the previous public hearings, it is imperative to get certified voting systems to the field as quickly as possible in a manner that doesn't impose unnecessary costs. With that, I cannot stress enough the importance of having standards that are as unambiguous as possible to help accommodate these needs. For VVSG 1.0, there have been over 20 Requests for Interpretation, RFIs, that were opened due to the ambiguity of many of the requirements. This may not seem like a significant number to some, but this is a very tedious and time-consuming effort that involves parties from both labs, the manufacturers and the EAC and can hinder the process of getting voting systems through the test and certification program in an efficient and timely manner. Having standards that are clear and as precise as possible also prevents inconsistencies in testing among the Voting System Test Laboratories. I more than appreciate the time and energy that has gone into developing the proposed VVSG 2.0 Policies and Guidelines, but I would like to respectfully request that modifications be considered to reduce the ambiguity in the manner that these have been written. I certainly understand that the Principles are to provide high level system design goals and that the Guidelines are to provide a broad description of the functions that make up a voting system, but in my opinion there needs to be some level of specification in order to write the requirements and test assertions. Terms like trustworthy, clear, meaningful, robustly and gracefully can all be interpreted differently and cannot be objectively verified. What's clear and meaningful to me, may not be to someone else. As I said earlier, SLI has not seen the requirements that have been developed to date and perhaps they have been written in a way that addresses the ambiguities in the Principles

and Guidelines, but it's hard to say without having seen the requirements or the test assertions. In the past versions of the standards, ambiguity has been an issue.

If I may, I'd like to make one additional comment or request. If my understanding is correct, the requirements are to contain the technical details for manufacturers to design their voting systems and the test assertions are supposed to contain technical specifications needed by the labs to test the voting systems against the requirements. If this is the case, I feel it is important to have early communication with the VSTLs regarding the development of the requirements and test assertions, perhaps, most importantly the test assertions. SLI was asked to assist with the development of test assertions for VVSG 1.0 2005. We were very involved with the creation of test assertions written to address ambiguities that were realized after implementation. We have not participated in developing test assertions for the VVSG 2.0, which is a bit concerning considering that the primary reason for developing test assertions is to assist the test labs. I feel the assistance that SLI provided in the past was very valuable. In fact, Mark Skall, who worked for NVLAP at the time and headed up the effort of creating test assertions, emailed me personally to thank the SLI team, in particular Mike Santos, for the invaluable support and commitment in developing thorough and clear test assertions that aided in the prevention of variances in test procedures.

Once again, I appreciate the opportunity to provide a statement today. I feel that the development of the VVSG 2.0 Principles and Guidelines along with the requirements and test assertions must be done right the first time. I believe we have had plenty of opportunity to learn what has worked well and what has not. I certainly don't have all the answers, but I do feel that precise principles, guidelines and requirements will help to make this next round of standards more effective and prevent needless inefficiencies. I more than appreciate you listening to my feedback and I'm happy to answer any questions that you may have.

Thank you.

Recipient Information

To: Brian Newby, Executive Director
Company: U.S. Election Assistance Commission
Fax #: 13017343108



Sender Information

From: Robert Rutkowski
Email address: r_e_rutkowski@att.net (from 23.115.46.18)
Phone #: 7853799671
Sent on: Thursday, May 30 2019 at 2:42 PM EDT

Brian Newby, Executive Director
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910
Phone:866-747-1471 (toll free)
or 301-563-3919
Fax: 301-734-3108
<https://www.eac.gov/contact/>

Re: Ban wireless modems and internet connectivity in the federal guidelines

Dear Executive Director Newby,

By close of business yesterday, more than 50,000 citizens from across the political spectrum will have called on the EAC to help secure the vote by banning wireless devices and internet connectivity in voting equipment certified by the federal government.

The action is taking place as part of the official comment process on the new Voluntary Voting System Guidelines, which the EAC is charged with issuing. The guidelines influence the design and manufacture of voting machines that the public uses in federal elections. Although the federal guidelines are voluntary, many states require voting systems to adhere to them.

After the 2016 elections raised questions about the integrity of U.S. election systems, it often was stated that voting systems could not be remotely attacked because they are not connected to the Internet. However, some voting systems include cellular modems to be used to communicate election results at the end of election night and other purposes. Public telecommunication networks communicate over the internet at points; the modems create an attack vector that hackers can exploit to compromise the voting system, install malicious software and tamper with election data in current or future elections.

Many states ban the use of wireless modems because of the grave security risk they pose, but several still use voting systems with wireless modems. Those states include Florida, Michigan, Minnesota, Rhode Island and Wisconsin.

Advocacy organizations – including Public Citizen, the National Election Defense Coalition, Common Cause and FreedomWorks – have alerted their members of the need for citizen comments supporting a ban on wireless modems and Internet connectivity in the federal guidelines. More than 50,000 citizens responded and sent comments to the EAC on the subject.

Our country is still waking up to the threat posed to our democracy by hacks and computer error.

People are ready to push our government to secure the vote. The public support for banning wireless modems in federally certified voting machines is overwhelming. Tens of thousands of people took action during a holiday week to call on an agency they had never heard of before to fix this.

Banning wireless modems is a commonsense measure to ensure the integrity of our voting machines. There is broad grassroots support for taking such a step to secure our electoral infrastructure. The process for submitting public comments is complicated enough without shifting the goalposts at the last minute. I hope the EAC will still hear what the grassroots in this country have to say and strengthen the integrity of our elections.

Citizens are acutely aware of the need to secure our election systems. They understood immediately that putting a wireless modem into our voting machines and vote tabulation systems greatly expanded the opportunities for sophisticated actors like North Korea or Russia to wreak havoc with the vote counts.

For too long voting system vendors have distorted the threat and muddled the issue of using wireless modems by claiming that they don't expose systems to the internet, but that just isn't the case. The American voters need the U.S. Election Assistance Commission to acknowledge and address this significant threat to election system security by banning wireless modems and internet connectivity in the federal guidelines.

Yours sincerely,
Robert E. Rutkowski

cc:

Representative Steny Hoyer
House Majority Leader
Legislative Correspondence Team
1705 Longworth House Office Building
Washington DC 20515
Office: (202) 225-4131
Fax: (202) 225-4300
<https://www.majorityleader.gov/content/email-whip>

2527 Faxon Court
Topeka, Kansas 66605-2086
P/F: 1 785 379-9671
E-mail: r_e_rutkowski@att.net

This fax was sent using the FaxZero.com fax service. Please send your response directly to the sender, not to FaxZero.

FaxZero.com has a zero tolerance policy for abuse and junk faxes. If this fax is spam or abusive, please e-mail support@faxzero.com or send a fax to 855-330-1230, or phone 707-400-6360. Specify fax #24533585. We will add your fax number to the block list.



DISABILITY
LAW CENTER

Your rights matter.

Voluntary Voting System Guidelines 2.0 / Public Comment

May 29, 2019

Sheri Newton / Voting Access Director

(435) 232-4269 / (800) 662-9080

snewton@disabilitylawcenter.org

Dear US Election Assistance Commission:

The Disability Law Center is Utah's Protection and Advocacy agency. In accordance with our federal mandate to "ensure the full participation in the electoral process for individuals with disabilities, including registering to vote, casting a vote, and accessing polling places" under the Help America Vote Act, we are the leading expert on access to the vote for Utahns with disabilities.

The DLC appreciates the Election Assistance Commission's (EAC) effort to balance the need for access and security. However, we're concerned about an emerging conversation around returning to paper ballots. This movement puts Principle 6: Voter Privacy in peril. Without alternatives to hand-marked ballots, a voters right to a private and independent vote is at risk. We ask that any EAC recommendations at a minimum regard a ballot marked by hand or by a ballot-marking device as a "marked paper ballot." Guidelines should include requirements for the usability of both types of paper ballots.

The DLC supports VVSG 2.0 Principal 7.1 and concurs with EAC advisory board member Dr. Philip Stark that the voter should have some control over the presentation of information for the purpose of making his or her selections. Currently, many ballot-marking devices do not allow the voter to increase text to an adequate size, audio instructions for using the keypad to navigate a ballot on the screen can be complex and hard to remember, and the keypad may not follow the standard layout to which many voters who have low vision or are blind are accustomed. We suggest evaluating the voting system to determine if its operation is intuitive and consistent with accessible systems used by voters and poll workers for other daily tasks. Testing must ensure that the system accurately captures voter intent and verifies selections by the full range of voters and election workers, including those with disabilities.

Until fully accessible and reliable paper ballot voting systems are widely available, we should remember that security and accessibility aren't mutually exclusive. In fact, they should be highly prioritized when selecting a voting system. As such, the DLC endorses Dr. Stark's recommendation that VVSG 2.0 emphasize the importance of each voter having a way to mark, verify, and cast a ballot that is as independently usable by him or her as possible. We also agree the guidelines should state that he or she have a way to independently verify that the paper record matches his or her selections.

The DLC shares the National Disability Rights Network's worry that VVSG 2.0 will lead to greater segregation of voters. In Utah, where voting by mail is state-wide, we've witnessed the impact for voters with disabilities. There are fewer opportunities for voters who cannot read or mark a ballot independently and an inherently segregated voting experience. With fewer polling places and fewer machines, poll workers have misconceptions about who may use the devices, they have trouble describing or activating the accessible features, they segregate voters who use the machine by setting it up in a separate area from other voting, and election officials make no effort to inform voters of the option to use a voting machine. This is why it is distressing that comparability requirements are not included in VVSG 2.0.

Fortunately, there are more possibilities. The Vote at Home movement is growing in popularity, and we have seen how vote-by-mail is increasing electoral participation across the board. Unfortunately, because of an almost complete lack of accessible options, it still requires many voters with disabilities to rely on others or hurdle obstacles that non-disabled voters don't encounter, like securing transportation or leaving work. This is why it is disappointing that VVSG 2.0 largely does not apply to nontraditional voting systems. A voting system must include accessible options for voting in the same manner as everyone or else we are furthering a separate and unequal voting system.

There are other solutions, too. We should look more closely at the possibility of electronically-fillable and printable ballots. Another option may be a system like VOATZ. VOATZ enables any voter to cast a ballot using her or his tablet or smartphone. This means voters with disabilities can use the same assistive technology that works for them every day. It also uses blockchain to ensure each vote is secure and auditable. We assert that such systems are consistent with VVSG 2.0 Principal 5: Equivalent and Consistent Voter Access and they effectively mesh accessibility and security.

Given this and other technological advances, we can and must have secure and accessible elections. As the EAC crafts guidance, it is imperative that they encourage states to incentivize the purchase of systems which have equal access and allow each and every voter to securely cast a private and independent ballot. Americans deserve, and will accept, nothing less. Thank you for your time and consideration of our perspective.



May 29, 2019

Chairwoman Christy McCormick
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, Maryland 20910

Dear Chair McCormick,

Since their establishment in the Help America Vote Act (HAVA) of 2002, the Voluntary Voting System Guidelines (VVSG) have played a crucial role in shaping the voting equipment used in the U.S. by addressing aspects of functionality, accessibility, accuracy, auditability and security. Though voluntary, the VVSG influence the voting system market and impact State certification, even in States that do not formally require certification of voting equipment by the U.S. Election Assistance Commission (EAC). We thank you for the opportunity to comment on the VVSG 2.0.

New VVSG Format

With the development of VVSG 2.0 the EAC and the Technical Guidelines Development Committee reimagined the VVSG to be a set of high-level, plain language principles and guidelines that is intended to be accompanied by a separate document defining the requirements voting systems must meet to comply with those principles and guidelines. This is a radical departure from the previous structure of the VVSG which included voting system requirements *with* the guidelines. The new structure allows the guidelines to be accessible to and easily understood by a greater number of stakeholders and may prove advantageous in other ways. However, under the new structure, with the requirements no longer included in the VVSG, the path for adoption of the requirements is no longer specifically dictated by HAVA. By separating the requirements from the VVSG the EAC has created a new article which lacks a defined policy for development, comment and adoption. Furthermore, the new structure puts an immoderate amount of importance on the voting system requirements which must provide a high level of detail and specificity to determine if a system complies with the VVSG. The lack of published policy regarding the Commission's handling of the requirements introduces opacity and uncertainty to this very important component of the VVSG. **We urge the Commission to define and publish the policy for the development and adoption of the voting system requirements as soon as possible.**

The Importance of Prioritizing Robust Security Provisions in the VVSG and its Requirements

As the U.S. faces an unprecedented threat to the integrity of our election systems and grapples with strategies to protect election infrastructure, there is increased reliance and expectation that the VVSG will provide that voting machines are resilient and secure. It is important that the VVSG deliver meaningful and effective guidance and requirements that will improve the security of voting systems and lessen exposure to manipulation, tampering or hacking. In some cases, this will mean States may need to implement new administrative procedures or practices in order to adopt voting equipment with more robust security profiles that comply with the VVSG 2.0 – this is not a bad thing. The VVSG should aim to provide a framework States can adopt to improve their security and fortify their devices against potential cyber attacks, which may require abandoning less secure practices. In developing the VVSG and the VVSG requirements there may a temptation to omit an important and necessary security provision that may conflict with some States' current administration practice, essentially diluting provisions in order to accommodate an existing, perhaps outdated, protocol. We think this would be a mistake – the VVSG and requirements must provide ambitious and meaningful security provisions and should not be weakened to accommodate existing protocols and practices which may not be safe. Moreover, the VVSG are voluntary; States can opt out in whole or in part according to their needs. It would be ill-advised to weaken the VVSG and its requirements as a whole in order to accommodate individual State's administrative practices.

Specific Comments

The VVSG 2.0 reflects a careful, thoughtful, sensible and thorough set of guidelines for voting systems and we commend the EAC and Technical Guidelines Development Committee for their efforts. Overall, we strongly support the VVSG as drafted and urge inclusion of one critical additional Guideline to prohibit the use of wireless modems and internet connectivity in voting system.

We respectfully offer the following comments on specific provisions for your consideration.

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

We support this Principle and its Guidelines but we believe it could be strengthened and clarified to add to Guideline 3.2 "and election records" and "and in a form." [Additions below in red.]

*3.2 - The processes, and transactions **and election records**, both physical and digital, associated with the voting system are readily available **and in a form** suitable for inspection*

In order to achieve meaningful transparency, not only the processes and transactions should be available for inspection, but also the various reports and ballot records.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

We strongly support this Principle and its Guidelines in current form. Lack of interoperability has limited election administrators' options for voting equipment. If a jurisdiction currently uses one vendor's system, administrators are unable to purchase elements of the election system from another vendor, even if that vendor's product may better meet the jurisdiction's needs. Additionally, in order to

implement effective, efficient audits it may be necessary for the audit software to parse exported results and cast vote records.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results

We vigorously support Principle 9, Guideline 9.1 and the associated Guidelines requiring Software Independence and auditability in voting systems and applaud the Commission and Development Committee for including this vital security provision.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Again, we strongly support Principle 10 and Guidelines 10.1 and 10.2 and commend the Commission and the Development Committee for its foresight to provide robust protections for ballot secrecy in voting equipment. As the Development Committee considered this Principle carefully, it noted that some States' practices run contrary to this Guideline, however, it also decided the need for strong protections for ballot secrecy outweighed the possible conflict with that small number of States. We strongly agree and urge the Commission to ensure this Principle is maintained and supported by effective requirements.

Principle 13: DATA PROTECTION

Given that our election systems are being targeted for interference through cyber attacks, we believe it is imperative the VVSG also include a prohibition on connectivity to the public Internet through wireless modems or other means. Therefore, we strongly urge the Commission to include as Guideline 13.5 under Principle 13: DATA PROTECTION:

"Guideline 13.5: The voting system does not use wireless technology or connect to any public telecommunications infrastructure."

Though it is widely held and frequently repeated that voting equipment is not connected to the Internet, many voting devices employ wireless modems which use IP addresses and IP packets that transmit over

the public Internet. Wireless modems introduce a host of security risks that were outlined in a [letter](#) to the EAC in 2018 signed by over 30 noted computer security and election integrity experts.

Some election management systems are hosted on devices that are used for multiple tasks that require Internet connectivity. Some vendors have installed remote access software on the election management systems to enable them to remotely manage election procedures and data.

There are many States that already incorporate provisions in their election system requirements and administrative rules that ban wireless modems and internet connectivity, this is not universal and many States don't ban connections to the Internet or the use of wireless modems. These dangerous practices greatly increase the exposure of these voting systems to cyber attacks and should be explicitly proscribed by the VVSG even if they will conflict with some States' existing practices. This is an opportunity for the VVSG to compel better safeguards and security and should not be weakened to tolerate poor election security practices.

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

To further strengthen the provisions for System Integrity, we urge the inclusion of the following Guideline 14.5 under Principle 14: SYSTEM INTEGRITY:

"14.5 The voting system will detect, and will not permit access by or connection to, any digital storage device that incorporates or contains executable code."

Election administrators, stakeholders, elected officials, lawmakers and the public hold expectations that the federal VVSG provide a strong, effective framework for secure, accessible, trustworthy voting equipment. We support the VVSG with the inclusion of a prohibition on wireless modems and internet connectivity.

Thank you for the opportunity to comment on Guidelines.

Sincerely,

James A. Hendler

Susan Greenhalgh

Chair

Policy Director

U.S. Technology Policy Committee of

National Election Defense Coalition

The Association for Computing Machinery

cc. Brian Newby

Executive Director

U.S. Election Assistance Commission

Voluntary Voting System Guidelines 2.0

In what follows Free & Fair's input to this VVSG 2.0 document is written in red.

These comments were written by Joe Kiniry with input from Dan Zimmerman, Joey Dodds, Rod Chapman, and Luke Meyers at Free & Fair and Galois in May and June of 2019.

Principles and Guidelines

We suggest that every domain term used in this document must be precisely defined in the VVSG 2.0 or NIST information security glossaries. Currently there are several terms used that are not defined. We highlight these terms as they occur

Principle 1: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly-accepted election process specifications.

1.1 We presume that "...commonly-accepted election process specifications" is an indirect reference to said process and common data format specifications under development by NIST. If that is the case, it could be said more clearly. Also, we hold concern that "commonly-accepted" is under-specific—e.g., are IRV schemes commonly accepted?

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.2 We suggest that real-world operating conditions must include adversarial environments.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

1.3 We suggest "testers" is overly specific to outdated evaluation processes. We suggest "evaluators" so that it is clear that dynamic testing is not the only (or best) way to evaluate a system's conformance to a specification—static analysis and formal assurance are complementary critical evaluation technologies.

Principle 2: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

2.1 We suggest "systems development", not just "software development", given that voting systems include hardware, firmware, and software.

2.2 - The voting system is implemented using best practice user-centered design methods, for a wide range of representative voters, including those with and without disabilities, and election workers.

2.2 We suggest that it should be made clear if support for election workers with disabilities is mandatory.

- 2.3 - Voting system logic is clear, meaningful, and well-structured.
- 2.4 - Voting system structure is modular, scalable, and robust.
- 2.4 "Robust" is not a well-understood modifier describing system structure.**
- 2.5 – The voting system supports system processes and data with integrity.
- 2.5 "Integrity" is not a well-understood modifier describing system processes.**
- 2.6 - The voting system handles errors robustly and gracefully recovers from failure.
- 2.7 - The voting system performs reliably in anticipated physical environments.
- 2.7 We suggest that "anticipated physical environments" must include adversarial environments.**

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

- 3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.
- 3.1 Make clear that the audience of such documentation is an expert in the state-of-the-art, and not the general public.**
- 3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.
- 3.2 Who are the inspectors?**
- 3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

- 4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.
- 4.1 We suggest "interoperable" is not sufficient. We prefer "open common data format".**
- 4.2 - Standard, publicly-available formats for other types of data are used, where available.
- 4.2 We suggest "Open, standard, publicly-available...".**
- 4.3 - Widely-used hardware interfaces and communications protocols are used.
- 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.
- 4.4 We suggest "...devices, hardware, firmware, and software...".**

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities, without discrimination.

- 5.1 - Voters have a consistent experience throughout the voting process in all modes of

voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify and cast their ballot or other associated cast vote record, without assistance from others.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

We do not know what "perceivable" means. We also suggest that there is a missing principle that focuses on "cast as intended" with some quantifiable metric, especially in the case of ballot marking devices.

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

We do not know what "safe" means in this context.

8.1 - The voting system's hardware and accessories protect users from harmful conditions.

8.1 What are "harmful conditions"? Electrical shock? Fear of reprisal from an abusive spouse?

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is measured with a wide range of representative voters, including those with and without disabilities, for effectiveness, efficiency, and satisfaction.

8.4 The voting system is evaluated for usability by election workers.

8.4 We presume this means "...the system is evaluated so that it can be used by election workers." The current version is ambiguous.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an

undetectable change in election results.

9.1 We think that this is the most important principle in this entire document in the face of nation-state adversaries.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2 We suggest that “correct” is ambiguous—perhaps “...correct insofar as it represents the will of the voters...”.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

9.4 We suggest that “efficiency” needs some additional exposition because it isn’t clear what the metric for efficiency improvement is meant to be. Is it calendar time? Election worker effort? Cost? We also suggest that the clause “...audits that are based upon statistically meaningful, evidenced-based science.” is necessary. This is important because current geographically-biased, non-random, small-scale L&A tests and post-election audits do not provide any statistically meaningful evidence for an election’s integrity or trustworthiness.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters’ ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter’s identity with the voter’s intent, choices, or selections.

Principle 11: ACCESS CONTROL

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - Access privileges, accounts, activities, and authorizations are logged, monitored, and reviewed periodically and modified as needed.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3 What does “strong” mean in this context?

11.4 - Default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION

The voting system protects sensitive data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

13.4 We suggest that such security properties are also relevant to all data stored on all devices, not just transmitted over a network.

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

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

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system employs mechanisms to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

Public Comment on the VVSG 2.0 Principles and Guidelines by Harvie Branscomb, 5/29/2019
<http://electionquality.com>

Uploaded at the eac.gov site in 7 parts. This is the complete document.

Major topics:

- 1) Need for VVSG
- 2) Transition strategy from 1.0 to 2.0
- 3) Relationship of P&G to Requirements
- 4) Relationship of requirements to test assertions or test procedures
- 5) Need for balancing of Principles
- 6) Scope of VVSG – need for clarity and eventual expansion of scope
- 7) Role of Glossary
- 8) Process to create P&G and Requirements
- 9) Process to coordinate Glossary
- 10) Process to create test plans
- 11) Decentralization of testing
- 12) Role of Commissioners in requirements and future P&G
- 13) Need for broad based review and input for update of requirements
- 14) Discovery, appeal methods for updating requirements
- 15) Defects and strong points of principles
- 16) Missed opportunities- effects of input from existing legacy vendors
- 17) Need for realistic interpretation of Guidelines
- 18) Relative need to support future v. existing technologies and methods
- 19) Inconsistencies with usage of “cast”
- 20) Inadequate and restrictive usage of the singular phrase “ballot”
- 21) Potential risk of nebulous definition of E2E
- 22) Potential risk of failure to fully support MMPB
- 23) Huge benefit of election record transparency
- 24) Claims that stand as obstacles to ballot transparency
- 25) Need to define substantive, not absolute ballot anonymity
- 26) Separation of systematic against self-identified risks to anonymity
- 27) Value in reduction of styles
- 28) Means to reduce styles
- 29) Potential risk of failure to fully support public transparency of records
- 30) Removing the fear of multiple sheet ballots
- 31) Conclusion- will we achieve the evidence based public election?

1) Need for VVSG

Manufacturers have historically guided policymaking on voting systems with innovation prior to regulation. Particular jurisdictions such as in Colorado and California have chosen to pilot and

then use these technical and procedural enhancements such as early voting, sometimes before all the integrity side effects have been explored. I live and regularly witness and verify elections using credentials in Colorado, one of these early adopter states. Colorado has worked with manufacturers to introduce new vote capture and tabulation methods. And at least since 2000 academics and activists and NGOs have coordinated to invent and gain regulatory support for integrity measures before manufacturers became involved, particularly the post election audit and then the risk limiting audit.

Meanwhile convenience-seeking partisans have introduced numerous voter-centric options that decrease obstacles to vote but rely more on technology rather than citizen oversight to maintain integrity – such as vote centers and mail-in ballot. The VVSG has provided a route for coordination of the many states with the few manufacturers to begin to achieve a semblance of pragmatic uniformity or at least a path towards it. VVSG 2.0 stands to be substantially more effective at bringing a potential Pandora's box of diverse innovation into a coordinated environment, perhaps without simultaneously presenting an obstacle to competition or innovation. The hope is that all of these goals will be achieved. In any case, self-regulation by voting manufacturers is highly unlikely to achieve adequate results, given the diverse characteristics of the various states and the vendors, as well as the potential for dramatic change in the way we vote and the way votes might be counted. Yes, the VVSG is crucial and it is crucial that it is formulated carefully to produce the desired result.

2) Transition strategy from 1.0 to 2.0

A clever strategy is needed to motivate vendors to design for not only a static VVSG 2.0 but a dynamic set of requirements that evolve over time. It is even more important that states will write laws to cause their certification requirements to track with the federal testing guidelines without diverging too much. Some ideas heard at the Silver Spring hearing seem strongly supportable. For example, the breaking up of requirements into chunks that can be tested and adopted at different times, with separate laboratories assigned to deal with categories of requirements. That seems sensible. Incremental progress towards full commitment to the latest standard could be allowed at the same time component testing and interoperability testing should replace the existing monolithic requirements and full system test scenarios now in place. The idea that component manufacturers might ask for pre-testing of select portions of the standards prior to asking for federal certification seems sensible and supportable. It is also key that the requirements not present an obstacle either to innovation or competition over the long term.

3) Relationship of P&G to Requirements

I favor the idea that Principles are more like constitutional provisions while Guidelines are like legislation and Requirements are like regulations. Test assertions if necessary or perhaps just test procedures should implement a means to measure success at fulfilling the requirements, as such Requirements must be sufficiently exact to be imminently achievable.

Clearly the Commissioners serve in the role of a constitutional convention to set the principles at the outset and to modify them as needed, presumably rarely. Probably the Commissioners with strong support from staff can adequately take care of the “legislative” level of Guidelines as well, but these deserve a regular such as biannual review.

Finally, the Requirements require both experience and expertise and foresight to be able to achieve the necessary pragmatism, applicability and completeness. Update of Requirements will be needed on a regular basis, at least with annual opportunity for initiation of change including from unexpected sources. Something like a review board is needed to periodically assess the success or failure of the requirements to fulfill the Guidelines, and less frequently the same for the Guidelines to adequately represent the Principles.

4) Relationship of requirements to test assertions or test procedures

The transliteration of Requirements to Test Procedures can be undertaken by subject matter experts appointed by the Commission to include reasonable oversight and review by EAC staff. The categorization of the requirements and tests into separate domains that can be served by subject-specialist laboratories can also be done by this group. Further subsets of requirements/tests could be created to allow incremental adoption of the standard to ease the transition for manufacturers.

5) Need for balancing of Principles

Fifteen principles have been identified and are about to be adopted as the constitutional foundation for voting system testing that maintains the quality and credibility of tabulation for the national election ecosystem. It is crucial to recognize that these are not orthogonal or independent and they ought not be intended to be equally prioritized. Some elements of some principles act in opposition to elements of others. The EAC will be required to assess and promulgate as policy a means for the interacting principles to be balanced. This may be the most difficult of tasks for the Commission. Likely it is a continuing endeavor that requires assessment of the result of the balancing.

6) Scope of VVSG – need for clarity and eventual expansion of scope

The current understanding is that VVSG scope is limited to “voting system” and that is arguably limited to ballot design, ballot creation and contest option presentation, capture of selections by voters, interpretation and adjudication, recording of cast vote records, tabulation, reporting of results and auditing. It is a fact that this set of functions does not describe the election system. Nor does the quality achieved in these functions necessarily result in a credibly correct election. Remote voting options and central count scenarios have caused the above list to be sadly insufficient. Questions remain about the applicability of the VVSG to the presumably voting system functions of remote ballot delivery, electronic marking, verification and electronic return. While the draft glossary contains terms to characterize these functions, the requirements as yet are silent with respect to them.

Moreover, there are whole portions of election process outside of vote capture and counting that are ignored by the current VVSG. For example the process of determination of eligibility of selections cast by remote voters is untouched. This process is increasingly implemented with unregulated complex programmed devices that both manage and perform signature verification. These devices are connected at least periodically by internet to voter registration databases. And there is increasing use of internet and similar mechanisms to register to vote and to collect signature samples for eligibility determination. These topics are ripe for inclusion in the VVSG voluntary standards and EAC certification testing in the future. The protocol for enhancement of the VVSG must come to include these topics.

7) Role of Glossary

The glossary is the substrate of the Principles, Guidelines and Requirements. It will glue together and make sensible the many diverse requirements and will avoid uncertainty as to meaning. Much work has been done to create unique standalone phrases to distinguish the many phases, items and entities within elections. Effort has been made to avoid confusion about terms such as the multiple meanings of “contest.” In VVSG 2.0, contest means “a single decision or set of associated decisions being put before the voters” and does not refer to the legal challenge of an [election](#) outcome.

There remain however some words that are used in competing contexts that do yet need clarification. I have been studying this topic for months and communicating with our State Audit Working Group that meets weekly to arrive at suggestions to provide to the EAC working groups. Now that a complete draft document of about 270 pages has been released this has become possible. There are dozens of places where definitions can be tightened, and requirements can be updated to use the correct phrase from the Glossary. There are places where new phrases need to be added to avoid confusion of multiple meanings. For example, the phrase “ballot image” was defined to be an electronic record of all votes cast by a single voter. This definition is contrary to the common usage that refers to a depiction of one or more sides of a paper ballot. It ought to be defined that way in recognition that a cast vote record is substantially different. However, the phrase “ballot image” also isn’t yet used within VVSG requirements and that suggests that improvement to requirements is yet needed to address that topic. There are numerous cases of important phrases in the Glossary not yet used in requirements that serve as a flag to remind us that additional work on Requirements is still needed.

8) Process to create P&G and Requirements

This brings up a need for brief discussion of the process by which the Requirements came about – the public working groups should be able to bring in both existing vendor experience and also the needs of future vendors and innovators and academics and election quality advocates who are seeking policy that will define and improve election integrity. The process used to reach the current VVSG draft was far superior to previous efforts. One problem with it is that it is slow to reach a draft and slow to share it beyond a few people on a single phone call. If the drafts could be shared instantly and constantly between all stakeholders (in reality the public) then response to observed defects could be much faster. If there seem to be stakeholders

advocating opposing positions who cannot find a compromise, then the issue needs to be escalated to a more refined process that will eventually reach the Commissioners for a policy decision. Above all, it is essential that the participants in the process of developing requirements not be curtailed beyond where it is today. If anything the process should be opened to more participants.

9) Process to coordinate Glossary

The Glossary is crucial to a well understood set of Requirements. At present there are several terms that are being used for entirely different meanings that are easily confused and must not be conflated. For an example, and perhaps the most important case is the use of the word “cast” that is already well defined in the Glossary as a voter action. But in the draft requirements (yet to be finalized) the word is also used for a clearly system related action that really ought to be known as “acceptance” rather than “cast.” In this instance, the Glossary is fine but the phrase “accepted ballot” must be added to the Glossary and the word used for the system-centric contexts where “cast” is currently found.

A different instance is the case where the definition is nebulous but the meaning of the usage is consistent and clear. In this case the Glossary definition needs to be updated to be more clear. The phrase “ballot image” is of this type. The current definition of “ballot image” includes all digital representations of voter intent including visual and cast vote records. It ought to be clarified. The EAC should take care to be sure that these types of instances are take care of. To do this each word in the Glossary needs to be checked to see if it is properly used in the requirements and in the Principles and Guidelines. In many cases I have found the words in the Glossary are not yet used in the draft at all. For a number of these, it seems likely that the requirements should include reference to very important concepts. In other cases, the Glossary can be trimmed to remove the words and phrases. The appropriate process for this improvement of the Glossary is to take each word and locate its usage in the drafts and then decide if any action needs to be taken. Those of us who are looking at the Glossary are attempting to conduct this research for key words that matter to our area of expertise. The results of that work can be made available to the NIST coordinators and the working groups as appropriate and we shall endeavor to do so.

10) Process to create test plans

One of the less discussed topics is how the test plans will be created – but this discussion did take place in Silver Spring. It seems clear that “test assertions” may not be a needed as an intermediary step between requirements and test procedures. If enough care is taken in writing the requirements, the test procedures can be created in a direct relationship with each requirement. This will however require enough specificity and clarity of each requirement- and that means they should be written in a direction and with an intention to be turned into quantitative metrics.

11) Decentralization of testing

A correlate to the decoupling of the standards to allow for component testing is a decoupling of test procedures into specializations. As made clear in Silver Spring, it does not make sense to expect a test lab to be proficient at testing all modalities of voting system function. Please do explore ways to separate different proficiencies into separate labs. Also it makes sense as suggested in Silver Spring to have a pre-test opportunity that is entirely optional to the vendor and can be accomplished at any time prior to the onset of final certification test. Also the results of these pre-tests should be applicable to the future certification decisions if appropriate.

12) Role of Commissioners in requirements and future P&G

I believe it is a mistake to remove the Commissioners entirely from the path to decide the requirements and the test plans. This is because inevitably policy decisions must be made – even decisions that appear to be substantially technical in nature. Without a stable administrative decision-making capability, some requirements may end up crippled by excess influence by some faction of stakeholders such as the vendors who have existing investments and may exert pressure for retaining the status quo.

13) Need for broad based review and input for update of requirements

What is obvious in the requirements that are in the draft today is that they are already inadequate to test devices and processes already being sold to election jurisdictions. And there are limitations built into the requirements that will cause problems for jurisdictions that are faced with the need to use multiple sheet ballots and who are moving toward remote voting and central count. These topics will be discussed separately. But the net result of the observation is that the requirements will need frequent review and improvement and a broad spectrum of influences will be needed to prevent the requirements from just reiterating existing designs and procedures familiar to the vendors and to officials with more simple election environments than others. We in Colorado have been at the edge of the state of the art now for a few years and are seeing side effects of innovations that need to be accommodated in the requirements. The EAC must prepare a system to evaluate the quality and fit of key requirements and subject these to excellent, frequent, broad-based oversight.

14) Discovery, appeal methods for updating requirements

It makes sense to have a periodic review of the pragmatic effect of existing requirements, both those recently put in place and previous versions of VVSG that may still be the target of testing. Obviously any deprecation of previous requirements will be resisted by manufacturers at least until they decide to end of life the last system that depends on it. This will present serious policy concerns that the Commissioners will have to administrate. On the other hand, requirements that as written stand in the way of innovation or simply are seen as obstacles to more efficient or better implementation of the principles and guidelines must be identified and

treated to a reasonable process for updating that will not interfere with existing designs for a reasonable period of time. None of this seems simple to implement, yet it is important to have such a process and it must not be dominated by any specific group.

Obviously the politics of this topic are not aligned along traditional partisan lines, but rather have pockets of entrenched support by groups such as those who place disability accommodation above all other goals as compared to pragmatists who look for solutions that satisfy 95% of the population best, compared to those who seek least common denominator solutions that attempt to serve 100% and may not succeed in doing so. Commissioners will need to resolve a means to address these real differences in a way that is both sensible and reasonably equitable. And where the rubber meets the road is in the writing of the requirements. At present the principles and guidelines will not serve to provide this administration because prioritization of the principles as they become requirements will be needed. It will serve the best interests of the public if the process of balancing principles is done in public with full attention to the side effects of decisions made.

15) Defects and strong points of principles

One strong point of the principles and guidelines as written is that they probably adequately span the range of issues raised by the needs of voting systems where voting systems are confined to vote capture and tabulation. Ironically a weak point is that the scope under consideration does not include eligibility determination meaning the process and equipment involved in determining the set of ballots to be tabulated. It is essential that a future version of VVSG or an equivalent will pay attention to systems for voter check-in, eligibility determination by signature verification, etc. These are already highly computerized systems that have the potential to degrade election accuracy by poor quality design or implementation including lack of sufficient security and auditing mechanisms.

Another potential weak point is possible excess attention to security where security means primarily the blocking of access. The voting system credibility depends substantially on excellent transparency. Transparency is a major principle, but the guidelines associated with it are deficient. They seem to attend largely to the documentation of the voting system rather than the potential for public access to election records including ballots and their correlates as well as reports. This may be a reflection of the extra attention to potential Russian interference, but regardless of the reason, the effect of over-attention to security was seen in Colorado in the aftermath of the Conroy v. Dennis case and since then much more attention has been paid to accuracy and auditability of the systems as well as the potential for beneficial public access. Security provisions initially introduced after the Conroy v. Dennis decision have been moderated to account for the realities of election process. The VVSG should not go overboard in a similar manner in the aftermath of accusations of Russian interference. Commission policymaking may be needed to ensure that meaningful transparency retains its crucial place in the operation of the election ecosystem.

16) Missed opportunities- effects of input from existing legacy vendors

A read through the requirements suggests to me that there is already an embedded bias towards electronic voter intent capture in place of pre-printed ballots that are intended to be hand marked. This seems odd considering that preprinted hand marked ballots are the standard voting method in many if not most states and all mail ballot states. Vendors who sell ballot marking devices have recently been effectively marketing their electronic capture devices as a substitute for hand marked paper (e.g. Georgia) and this direction seems to be already perhaps too much reflected in the writing of many of the guidelines and the requirements as well. An example is

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

The original text of guideline 7.1 is obviously focused entirely on an electronic vote capture method, ignoring the comparable needs of a preprinted paper ballot. The State Audit Working Group proposes to improve Guideline 7.1 to add “ballot design and any” to “default system settings for displaying the ballot” to correct for this apparent bias against hand marked paper. There are comparable omissions found in the requirements as well. It is essential that the Guidelines not be written with a profit motivated bias, and important that the requirements to follow also do not contain a preference for electronic capture over hand marked paper.

Another problematic trend in the Guidelines and Requirements is an apparent preference for absolute and perfect solutions to the very imperfect and unpredictable variations in voter ability to operate the voting system. This is represented in the phrases such as

Principle 7: Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

This sentence is idealistic, as perhaps a principle should be, but it is in reality unachievable – meaning that not “all voters” will be able to mark verify and cast a ballot that is perceivable, operable and understandable, and certainly not all will be able to do that independently of any assistance. So to be realistic, as the pragmatism requires, I join others in suggesting that the phrase “widest range of voters” be substituted, as is already present in the Guideline 7.1 that immediately follows.

Lastly the Guidelines and related requirements seem to treat transparency as if it is satisfied simply by rigorous pre-printed documentation, when the greatest benefits of transparency can be obtained by public access to election evidence that substantiates an evidence-based-election. For this reason I support others in adding the phrase “and election records” to “processes and transactions” in Guideline 3.2:

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available and in a form suitable for inspection.

This suggested improvement to add “election records” will allow for requirements that cause ballot designs and cast vote record formats to be conveniently and inexpensively redactable to protect ballot secrecy when needed- thus allowing for maximum transparency of the fundamental records of the election to the public who own them as public records in many states. Requirements should cause voting systems to be ready to copy and export election records suitable for public consumption for situations where state law allows.

Please ensure that the process by which requirements are finalized does overcome potential bias that exists because of the most frequent and steadfast participants in the working groups are members with a special interest.

17) Need for realistic interpretation of Guidelines

Guidelines that express ideals can be extrapolated into requirements that are impractical or are unrealistic. There are several of these that I can recognize but there may be others. As previously addressed, the ideal that all voters can vote both in privacy and with independence is very difficult to implement because of the diverse nature of the persons who will be wishing to vote. In some cases it may be easier for verification to be assisted by the voting system technology than for marking to be assisted. The Commissioners might find it reasonable to opine that independent verification is more important than privacy during marking. This kind of subtlety will assist manufacturers in serving the diverse public.

Likewise, election officials find it very challenging to determine what constitutes an identifiable ballot sheet. A realistic interpretation of privacy will distinguish between systematic impingement on privacy as opposed to voter-induced risks to privacy. Once again, policy can be expressed by the Commission that will assist in the creation of pragmatic requirements from the Guidelines. While such policies could be left up to the states and some perhaps will step up to address these finer points, it will immeasurably help the voting system industry to serve the public if the EAC Commission will provide consistency and sensibility to address implementation of idealistic goals expressed in the Principles and Guidelines.

18) Relative need to support future versus existing technologies and methods

There is a considerable time delay (not likely measured in months if not years) present in the decision-making process that results in new or changed requirements and finally the test procedures. Then a product intended to fulfill the new VVSG would require perhaps a full product design cycle and then prototyping, internal vendor testing and manufacturing. Then finally an actual certification testing cycle. Because this is a long time, vendors inevitably have a strong influence over what the requirements may look like as they will likely begin these innovation steps before the requirements are written. This isn’t an ideal situation because policy follows practice and that is opposite to the ideal order of things. There is also a natural danger that the requirements will tend to cause implementation of future voting systems to resemble what is currently experienced as a voting system by those in the working groups. An alternative that is much needed is to allow requirements to exist that are broad enough to

encourage development of innovative components for voting systems as some group of advocates have envisioned them. Both of these do make some sense, but there may be a need for encouragement of manufacturers and non-manufacturer innovators to bring better ideas to the EAC for inclusion in the requirements as early as possible for possible future components and systems.

Meanwhile there are already inconsistencies and obstacles to efficient and accountable and accurate systems already embedded in the draft requirements. In the following paragraphs I will address a couple of the most significant.

19) Inconsistencies with usage of “cast”

Inconsistent usage of the key word "cast" creates ambiguity. "Cast" according to the Glossary is voter - centric, an action taken by voter. This is very sensible and should be retained. But usage in the VVSG 2.0 draft requirements in probably twenty other places refers instead to a system-centric action that ought to be referred to as "accepted" e.g. "accepted ballot" in place of "cast ballot." Other possible words to use to replace the system-centric meanings of the verb cast are: to "read" or to "count" or to "tabulate". In some places "cast" is clearly used to refer to the step that creates the CVR. This step is definitely not a voter action and not consistent with the Glossary definition. The appearance of "cast" within the three word phrase "CVR" is also sadly inconsistent, but by now unavoidable.

I recommend to use the word "cast" (noun and adjective) to refer to the voter centric event as currently defined. Then introduce a different defined word such as "accept" and "accepted" to differentiate the system-centric usage from the voter-centric. In some places, the word "counted" or "tabulated" is more appropriate than "accepted." After casting, these system-centric actions deserve unambiguous labels. "Cast" doesn't belong in a requirement related to system functions after the voter is no longer involved. The provisional ballot presents a particular challenge. The current draft requirements use "cast" to refer to a decision taken after the system determines the eligibility of the already voter-cast ballot that is retained under identifiable cover. The challenge is solved by adding a concept of "pending acceptance" and then "accepted" status for a ballot pursuant to research performed well after casting of the anonymous ballot in an identifiable container.

20) Inadequate and restrictive usage of the singular phrase “ballot.”

The use of the singular word "ballot" is compatible with the election phase that takes place before and during the voter act of casting. Shortly after casting, an electronic ballot might likely remain as a single unit but a paper "ballot" may separate into separate sheets of which each are individually processed in scanning, interpretation, possible adjudication, recording as a sheet-specific entry in the cast vote record, and then subject to sampling for audit. These post casting events take place typically per ballot sheet, not per ballot. Reference to "ballot" as a unit during the post-casting tabulation phase is harmful because it implies that multiple sheets remain as a unit -even though this is very difficult for election officials to accomplish.

If the tabulator must report “cast ballots” (as current requirement drafts do specify) then the ballot must appear to the scanner as a unit even if the voter didn’t cast the complete set of sheets comprising the “cast ballot.” Remember that the scanner may not be facing the voter and will have no way to know what the voter “cast.” That situation then requires officials to fabricate missing evidence so that the full “cast ballot” is created by the time tabulation takes place. This is typically done by inserting “placeholder” sheets into any incomplete “sets of ballot sheets” prior to scanning. Treatment of a multi sheet ballot as a unit also may require draconian care in filling batches such as by increasing or reducing the length of batches to keep sheets together. Costly workload implications often pressure EOs to squeeze the contest options into a single and very long double sided sheet, creating high Ballot On Demand equipment costs and other disadvantages. Almost all references to “ballots” in tabulation ought to refer instead to “ballot sheets.”

21) Potential risk of nebulous definition of E2E

End to End is a concept that is already rolled into the VVSG draft as a separate track of requirements. This is likely to turn out to be a mistake, given so little experience with the concept at this date. Its current definition seems incomplete and unsuited to implementation:

cryptographic end-to-end voting system

A voting system that supports both voter verification and election verification.

This definition obviously relies entirely upon interpretations of “voter verification” and “election verification” and those in turn would rely upon a definition of “verification” none of which currently exist in the VVSG draft Glossary. Meanwhile, without further definition of E2E the label will be interpreted variously from time to time by various readers of the standards. E2E as an alternate voting method now exists within the VVSG as a route to avoid all the otherwise standard requirements. This suggests to me that the EAC is largely giving up responsibility for use of methods that could be labeled E2E. If so, then I hope the magic of encryption as implemented by the manufacturers does solve the many problems inherent in making and delivering a quality voting system. On the other hand, I doubt it. This alternate path through the future requirements seems unwise, while opportunities for smaller innovations might be blocked unnecessarily.

9.1.1-B – Paper-based or cryptographic E2E system

Voting systems must meet the requirements within the Paper-based System Architectures or Cryptographic E2E System Architectures section, or both.

Note here the voting system may be entirely certified under “Cryptographic E2E System Architectures” and not at all under “Paper-based System Architectures.” Apparently VVSG anticipates a new generation of paper-less voting systems certified under this separate route. At this point in time it seems premature to allow this much leeway under a federal voluntary standard. Permission to use supplementary encryption within a paper-based system to achieve

better “voter verification” or better “election verification” makes more sense, but definitions and standards for voter and election verification must be set first.

Here is one more example that clarifies that the E2E route is intended as an alternative to paper (from the discussion of requirement 9.1.1-A – Software independent):

There are currently two methods specified in the VVSG for achieving independence:

- *through the use of independent voter-verifiable paper records, and*
- *E2E cryptographic voting systems.*

The introduction of “E2E” as a separate path through the requirements as opposed to a supplemental path should be revisited.

22) Potential risk of failure to fully support MMPB

There are indications that well over 50 percent of voters today are voting by hand marking on pre-printed paper – referred to in the draft Glossary as Manually Marked Paper Ballot. I have observed that in multiple locations in the VVSG draft the applicability to hand marking of paper is missing in favor of attention to electronic vote capture interfaces. One example actually in the Guidelines is here:

7.1 - The default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

This Guideline clearly focuses on an electronic vote capture interface without applying the same intention to pre-printed paper as an interface. For that reason I and others have recommended to add the phrase “*ballot design and*” after “*default*” in Guideline 7.1.

There are apparently substantial differences of opinion about the relative benefits of electronic vote capture compared to paper. Without fully reiterating the arguments here, it might suffice to say that the Commissioners may have to intervene with a policy decision in order to be sure that manually marked paper remains a viable vote capture mechanism for future voting systems designed to meet the VVSG. The hand marked / machine marked argument represents another of the balancing acts that must be performed by the VVSG. In my opinion it is the success of meaningful verification of machine printed marks on paper to be tabulated that matters most in this very controversial division of perspectives. The large practical benefits of pre-printed, and if necessary printed-on-demand paper, argue strongly for keeping this vote capture method alive and well. And a well designed and implemented manual audit suffices to remedy the contribution to potential error in election outcomes that result from marginal marks that software cannot recognize. This has always been one of the biggest arguments against MMPB but the RLA or other well designed manual post election audit of paper solves that problem handily.

23) Huge benefit of election record transparency

Another sometimes overlooked potential value to be obtained from future voting systems is a fabulous opportunity recent scanner technology is already delivering but some state laws have yet to catch up. Modern tabulation devices produce both scanned copies of ballots and the associated cast vote records for purposes of review and comparison. Risk limiting audits conducted by officials require comparison directly to the physical paper ballot for very good reasons. In addition to election judges required to do the auditing, a few members of the public may be able to attend to verify the audit quality. But with current technology now being sold, after appropriate ballot secrecy safeguards are in place, and subject to local laws about access to records, any interested party could perform a virtual manual post election review to their own satisfaction at home – recognizing that there may be some misrepresentation of the paper by the images. This use of the ballot image is highly beneficial and can result in even higher accuracy of tabulation if the protocol for interaction of public with officials is well designed.

Unfortunately the Guidelines supporting the Transparency Principle do not yet refer to election records:

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available and in a form suitable for inspection.

I and others from the State Audit Working Group have proposed to add the phrase “*and election records*” to the above Guideline in order to enable requirements that will facilitate public access to records in a form that is inexpensive, efficient, and non-interfering and involving appropriate but minimal redaction to satisfy any local ballot secrecy provisions of law.

24) Claims that stand as obstacles to ballot transparency

In a paper system of vote capture there are three classes of voter intent records potentially available for some form of release such as publication online – the simplest is the cast vote record, then the ballot images and finally the paper itself. Claims have been made that a major risk to voter privacy in the general sense and ballot anonymity most specifically is publication of these election records. The argument goes that voters need proof to show the buyer or coercer to complete the transaction and the publication of the record satisfies this need. Even the cast vote record that contains no physical space to place an extraneous mark can, it is argued, be used to message to the coercer that the service has been performed. The most often voiced concern is called “pattern voting” and the method involves a guess by the coercer that a particular pattern of votes will not exist for a given style in the election. Then if this turns out to be true and the coerced voter does vote this pattern, then the coercer learns that the coercion has been successful. It is argued that this connection between proof and success at coercion amounts to enablement.

I question the validity of this assertion as speculation. The risk of deliberately lost privacy pales in comparison to other more systematic risks to voter privacy that result from poorly designed

or poorly executed election process. The mail ballot voting method itself offers ample opportunity for coercion of various types without the need for proof to be provided. A removal of the speculative channel to communicate with a coercer through the CVR doesn't remove the same channel on paper and ballot image – and election verification by human understandable media requires access from paper to image to CVR with adequate protection for voter privacy. I suggest removal of the definition of the unused phrase “pattern voting” from VVSG because other risks are larger and more damaging because they can be exploited by many more people. The bulk of the systematic risks can be resolved through well designed systems and practices guided in part through the VVSG.

25) Need to define substantive, not absolute ballot anonymity

The quest to achieve voter privacy takes two directions – one at the moment of voting and casting the ballot. In this case physical security is the primary tool to prevent access other than by the voter to the ballot being voted. The Principle of Voter Privacy is established to address this concern.

The provision of voter privacy with respect to the evidence of the vote is treated by the Principle of Ballot Secrecy. There is a virtual and one hopes physical chasm that separates these two regimes in election processing – one with full identifiability (with only very rare exceptions) of electors to determine eligibility; the other characterized by almost zero identifiability. In the former the scenario “his her or their” ballot remains appropriate. After casting, the pronouns do not belong – by then it is the public’s ballot and no one else’s. Any implication of personal ownership or association with the ballot should not be made, and certainly not in federal voluntary standards for voting systems. I hope the VVSG will conform to this distinction in use of pronouns- knowing that many of devices used and the events that take place that are subject VVSG requirements are in the latter post-casting regime – the anonymous one where “his her and their” should not describe a ballot sheet.

The medium for recording the vote (e.g. the preprinted paper) may exist prior to voting and casting and must still be designed to be and become anonymous, and after voting it must remain anonymous regardless of its further marking and its handling, meaning it cannot be associated with the identity of a voter other than for unavoidable reasons. “Unavoidable” is why I use the phrase “substantive identification” to describe a potent risk. After casting, the “ballot” may separate into separate sheets and each deserves separate treatment to ensure adequate anonymity. What constitutes “adequate” may be a controversial topic that requires policymaking by the Commissioners.

Absolute ballot anonymity (aka Ballot Secrecy) would if taken literally mean that the ballot may not contain DNA of the voter, fingerprints of the voter, or a recognizable tear pattern on the edge of the paper where the identifiable stub has been removed. These are mechanisms for associating a voter with a piece of paper that can be deemed unreasonable to implement and not worthy of systematic prevention. Other privacy risks involve intentional self-identification

by the voter such as cryptic patterns either within the contest option target or outside of it, and the previously mentioned pattern voting channel. These are methods under the control of the voter, would only be effective if deliberately used, and leave behind evidence of their use. These should not be considered “substantive” or “significant” forms of self-identification because their effectiveness is speculative and under personal control of the voter and are harmless if used only by the voter.

Substantive forms of self-identification are names printed on the ballot outside of a write-in region, signatures and initials – the type of self-identification that could be used by any observer to associate the ballot sheet with a voter. Substantive self-identification merits a systematic remedy in the form of a reasonable means of redaction at the time the risk is discovered. Voting systems could be better designed to detect substantive self-identification and as well to perform the necessary redaction -with copious opportunities for human oversight to prevent systematic obfuscation of voter intent that might occur at the same time.

26) Separation of systematic against self-identified risks to anonymity

Requirements related to Ballot Secrecy should distinguish between means of substantive self-identification as opposed to any means of self-identification that is unreasonable to expect the voting system to remedy. At the same time the requirements should differentiate between risks of self-identification from systematic risks to anonymity that are entirely the responsibility of the election system and its designers and operators.

Systematic forms of association of voter with a ballot sheet (out of control of the voter) deserve to be remedied in the design of the voting system as well as in its operation. Systematic risks to anonymity are applicable to solution via the VVSG requirements even though much of the risk is added by decisions to add special district elections to ballots. Rare styles are created when the added districts have borders that do not coincide with precincts and legislative districts already required to be on the ballot. Rare styles also result from voter options to choose vote capture methods that result in separate formats such as selections-only formats when full choice formats are prevalent or vice versa.

27) Value in reduction of styles

Rare styles result as unintended consequences of various recent enhancements to voting methods and in particular from voter convenience measures that involve options. Risks to ballot anonymity are aggravated by voter options about place and day to vote and also method of vote capture and medium of ballot return. These choices often affect both the format of the physical ballot sheet and the context in which that sheet enters the tabulation process. The decision to include on the ballot sheet districts that have ignored precinct boundaries generates as a side effect extra ballot styles often known as precinct splits. Some of these may easily become rare depending upon turnout with or without the voter options. Rare ballot styles in an

election are a primary mechanism for loss of ballot anonymity and the VVSG should promote voting system designs that minimize both the number and rarity of ballot styles. One way for future systems is to implement better ballot secrecy is by implementing ballot sheet styles for multi-sheet elections.

28) Means to reduce styles

Ballot sheet styles, meaning a separate ballot style per each sheet of a ballot (or corresponding portion of an electronic ballot) are not new, they are just hidden – every scanning tabulator that handles paper treats each sheet as a separate entity, and perhaps each side of each sheet as a separate entity. It is the EMS that typically assumes that each voter receives only one style in an election regardless of the number of sheets. This is actually a restriction that prevents solutions to ballot secrecy challenges and ballot style inventory challenges via intelligent pagination of elections onto multiple sheets that are allowed to be tabulated independent of one another. Even the highly speculative pattern voting risk is reduced with independent tabulation of ballot sheets. It would be wise for VVSG 2.0 to allow election jurisdictions to take advantage of this opportunity.

The division of district contests into two separate independent ballot sheets can resolve some systematic risks to voter privacy. Rare styles resulting from precinct splits sometimes produce a single unique ballot in an election. Contests for districts with inconveniently located borders placed on the same sheet may involve narrow intersections with few voters. Separation of incompatible contests onto a separate style sheet tabulated independently can provide a solution. This could be addressed in future VVSG drafts, including for VVSG 2.0.

A comparable means to reduce the number of styles and the number of rare styles is to make pre-election decisions about the contents of the ballot according to information to be provided by the voting system about risks to ballot secrecy based on the number of voters to be issued a given proposed style in an upcoming election. This is a service not unlike the intelligent pagination envisioned above that could resolve anonymity problems before the ballot sheets are printed.

Finally, the same information could advise legislation that creates special districts about the consequences of making their borders intersect inconveniently with already legislated borders for districts that are likely to share the same ballot sheet.

29) Potential risk of failure to fully support public transparency of records

If the VVSG serves its communities well, it will provide for means to achieve adequate anonymity to reasonably fulfill the principle of Ballot Secrecy. If so, the generic goal of voter privacy will be reached. And this achievement can and will happen in the context of an election system that provides for public access to election records such that there is little or no room for uncertainty about the outcome as determined by the process of interpreting and tabulating

ballot sheets. And if successful, these published records will be human readable and understandable and not the product of clever encryption schemes meant to hide any route to discovery of identity, and schemes that when they fail, may reveal far too much. Encryption serves well the purpose of providing what has recently been called "defensibility" of the administration of the election and its records – a way to prove that a record is identical to one that was originally subjected to a digital signature or the equivalent. This use of encryption is highly beneficial and will not stand in the way of public awareness of details of an evidence-based election.

30) Removing the fear of multiple sheet ballots

This version or another future VVSG revision could endeavor to protect election officials from the unnecessary extra costs and resulting fear of a two plus sheet ballot. Early steps to achieve multi-sheet benefits can be obtained by replacing the existing VVSG requirements on the "voting system" to report "cast ballots" with a requirement to report "tabulated" or "counted" "sheets" (assuming the ballot is on paper).

If that substitution is not made, a hidden side effect of VVSG is to favor the DRE, and the electronic ballot, and the selections-only printed electronic ballot image. In effect the VVSG will, perhaps unaware of the consequences, disadvantage a moderately sized inexpensive pre-printed hand marked full choice paper ballot sheet that many election officials now use and much appreciate. All of the above electronic examples, in contrast, naturally accommodate many contests in a single unit that could still be called a ballot in tabulation but paper is different. Multiple sheets of paper independently scanned and tabulated can provide real advantages. If the VVSG makes clear that the ballot (singular) is an identifiable item during eligibility determination and until casting, but beyond that, during all tabulation phases the ballot consists of sheets and what is to be measured and reported is how many sheets are accepted, read, interpreted, recorded, tabulated, etc. by sheet style. Of course if the ballot is a single sheet, you have a simple case still well covered by terminology.

31) Conclusion- VVSG 2.0 can help us achieve the evidence based public election

When the Commissioners and EAC staff acknowledge the many benefits of manually marked paper ballots and weigh in to make sure that they receive the attention they deserve –

and when transparency of election records is recognized as an essential goal, not uncompromisable but of equal importance to ballot accessibility to benefit the disability community and other principles-

-and when ideals in the principles- for example ballot secrecy- are not treated as absolute requirements that must be met even at the risk of public accessibility to election records for verification-

-and when Commissioners do carefully resolve other existing technical disputes with deliberate policymaking in the interests of the public at large-balancing one principle with prioritization with respect to another-

-and when states adopt these upcoming VVSG standards and manufacturers start building to the test specifications- in either order-

-then we can expect to see evidence-based elections beginning to happen in all conforming states plus a few more in jurisdictions.

Thank you for the opportunity to provide public comment on this most important topic.

GENERAL:

Concern: Confusion may exist around the purpose of the Principles and Guidelines document: that the Requirements and Test Assertions are used for testing, not these Principles and Guidelines.

Rationale: Many of these clauses are untestable and subjective, but can be reduced to testable requirements and test assertions as planned.

Mitigation: As part of the Commissioners' approval of these Principles and Guidelines, make a clarifying statement as described above.

CLAUSE SPECIFIC:

3.2 Concern: While "physical" processes lend themselves to the required inspection, "digital" processes include transactions occurring within microprocessors as well as myriad other processes that only instrumenting the device would allow for inspection.

Rationale: Allowing for inspection of every digital process in a voting system is impossible. Even if a device is instrumented, likely not every process can be inspected. COTS equipment in particular is not amenable to this concept.

Mitigation: While the concept of inspecting physical and digital processes and transactions is noble, it is impossible to develop a system that can meet even a favorable interpretation of the wording of this clause. Removing the "digital" language, especially when combined with the Principle calling for Software Independence (9.1) makes inspection of the digital processes unnecessary. In the alternative, digital processes can provide evidence via tools such as digital signatures that would provide assurance of the authenticity of their output. The language of this clause could be edited to require inspection of physical processes and transactions alongside the provision of evidence related to the output of digital processes.

3.3 Concern: This clause is directed to the "public" and not to the voting system, which could lead to misunderstandings by citizens with regard to what the system should output for inspection and how they gain access to those artifacts.

Rationale: Smartmatic supports public trust in elections and the opportunity for members of the public to be able to audit election artifacts intermediate to the process (such as machine programming file packages) and final outputs such as ballot images, audit logs, and results. Not defining who is the "public" and how they can access the voting system, which is required to fulfill this clause as written, can lead to misunderstandings and ultimately diminished trust by the very public this clause seeks to serve.

Mitigation: Language directed toward the voting system makes more sense here. A clause such as: The voting system will produce publicly verifiable outputs at each stage of the election, allowing members of the public to understand and verify the operation of the system throughout the election cycle.

8.2 Concern: This clause is unbounded with respect to the catalog of federal standards describing accessibility.

Rationale: Persons may attempt to place incorrect, improper, and unnecessary requirements on voting systems.

Mitigation: Add the word "applicable" to this clause to bound the range of federal standards.

8.4 Concern: This clause is phrased in a confusing manner.

Rationale: The clause, as written, can be confused to mean that election workers (aka Poll Workers or Polling Place Officials) must perform the evaluation of the voting system's usability.

Mitigation: Edit the clause to state: "The voting system is evaluated for election worker usability."

9.2 Concern: This clause seeks root cause information from the voting system, when the typical root cause of irregularity is outside the voting system.

Rationale: irregularities such as ballot accounting that cannot be reconciled or Election Night results that do not match audited or Canvassed results typically occur from human error, which the voting system is not likely to be able to discern.

Mitigation: The voting system is far more likely to be able to provide information regarding the **source** of irregularity rather than root cause, which is typically buried in a process. Edit this clause to reflect "source" rather than "root cause".

9.3 An editorial comment that the Software Independence aspect of the Principles and Guidelines (clause 9.1) *de facto* institutes paper based systems, which have the least resilience in the face of human error (voter or election official), malfeasance, and attack.

10.2 Concern: Voting systems complying with this clause will disallow automated processing of Provisional Ballots, as systems certified to FVSS and older VVSG's currently allow.

Rationale: Systems that allow the jurisdiction to append a Cast Vote Record with an identifier which can, after polls close, be used to pass or fail that Cast Vote Record and associated tallies based on State law "contain" and likely "produce" data that can, through jurisdiction processes, be associated to a voter. Enforcement of this clause will cause system architectures that place additional burden on election officials as they process Provisional Ballots.

Mitigation: Add to this clause "...except where needed to comply with statute, Rule, or established election processes and secured against unauthorized use."

11.5 Concern: The revocation required by this clause has no owner.

Rationale: It is not known whether this action need be automated or is expected to be manually performed by jurisdiction authorized users. If automated, how is the voting system expected to know in all cases when access revocation should occur?

Mitigation: Edit the clause to state that access is "revocable" when no longer needed.

14.4 Concern: Use of the word "administrator" may lead to unexpected consequences.

Rationale: in some places, the word "administrator" has a legal definition. "Administrator" may or may not be a defined access role in the voting system. Also, especially in large jurisdictions, a crew of persons (none of whom is an "administrator") perform firmware upgrades on the voting machines.

Mitigation: Keep the intent but avoid these possible consequences by making a "higher credentialled user" the role or person authorizing software updates.

Letter in response to request for public comment as published in Federal Register:
<https://www.federalregister.gov/documents/2019/02/28/2019-03453/proposed-voluntary-voting-system-guidelines-20-principles-and-guidelines>

to be emailed to: votingsystemguidelines@eac.gov delivered to EAC prior to 4PM May 29, 2019.

Dear EAC Commissioners:

Thank you for offering us the opportunity to comment on the proposed VVSG Principles and Guidelines and the accompanying Glossary. We, the undersigned, are members of the State Audit Working Group (SAWG). SAWG has been meeting regularly since 2008 to improve the accuracy of elections through post-election audits. We understand that a tremendous amount of work has gone into developing this document and we are reserving our comments for what we consider the most important suggested substantive changes and clarifications.

We the undersigned members of State Audit Working Group support the following comments specifically related to the Principles and Guidelines. We intend to submit separate comments at a later date about the Requirements and Glossary.

- Harvie Branscomb, Election Watcher in Colorado, electionquality.com, harvie@electionquality.com
- Duncan Buell, Commissioner, Board of Elections and Voter Registration, Richland County, South Carolina (affiliation for information purposes only)
- Sean Flaherty, Chair, [Iowans for Voting Integrity](#)
- Susan Greenhalgh, Policy Director, [National Election Defense Coalition](#), susan@electiondefense.org
- Celeste Landry, voting methods researcher and presenter, Colorado 2016 Presidential Elector
- Neal McBurnett, Election Integrity Consultant
- John McCarthy, election integrity advocate and retired computer scientist, JLMcCarthy@lbl.gov
- Kirstin Mueller, Election Security Advocate
- Stephanie Singer, Data Scientist and Former Chair, Philadelphia County Board of Elections
- Kevin Skoglund, Chief Technologist, Citizens for Better Elections
- Philip B. Stark, Associate Dean, Division of Mathematical and Physical Sciences, Professor of Statistics, University of California, Member EAC Board of Advisors
- Paul Stokes, United Voters of New Mexico
- Poorvi L. Vora, Professor of Computer Science, The George Washington University
- Luther Weeks Luther@CTVotersCount.org, CTVotersCount.org

and collegial organizations:

- on behalf of the [OSET Institute](#) & [TrustTheVote Project](#), Joy London, Esq. Associate General Counsel, OSET Institute, Inc.

Guide to annotation: Draft Guidelines are presented only for Principles commented upon; Guidelines are in italics; proposed deletion is shown as strikeout of red text unless otherwise annotated; additions are in underlined red text; explanatory commentary is indented and highlighted in amber.

Comments on the Voluntary Voting System Guidelines

Principle 1: HIGH QUALITY DESIGN (no comments)

Principle 2: HIGH QUALITY IMPLEMENTATION (no comments)

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes ~~and~~ transactions and election records, both physical and digital, associated with the voting system are readily available and in a form suitable for inspection.

We suggest changing Guideline 3.2 to add “election records.” It is not only the processes and transaction that need to be transparent, but also the election records including the various reports and ballot records. These election records are key for election officials administering elections, for voters voting in elections and for auditors using them as evidence for the quality of the overall election system.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

We strongly support this Principle and its Guidelines. It is critical for facilitating effective, efficient audits of election results. For instance, software to support efficient risk-limiting audits will need to parse exported results and exported cast vote records.

This principle should eventually lead to the ability to test components of voting system which would reduce the time and expense of voting system testing. After component testing, system integration testing will still be necessary for the final configuration of the system. Eventually, election officials should be able to swap components without repurchasing entire new voting systems. For instance, a jurisdiction might want to replace their BMDs or their scanners, without replacing the whole Election Management System. Having component level testing would allow new companies to enter the market in a specialized field without having to surmount the tremendous barriers of entire system development and certification. For example, companies that excel in providing interfaces for people with disabilities could enter the BMD market. Also, component testing probably would reduce overall certification times. We suggest that the EAC support the goal of moving towards component level testing in addition to system integration testing.

- 4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.
- 4.2 - Standard, publicly-available formats for other types of data are used, where available.
- 4.3 - Widely-used hardware interfaces and communications protocols are used.
- 4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS (no comments)

Principle 6: VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

- 6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.
- 6.2 *Voters can mark, verify and cast their ballot ~~or other associated cast vote record~~, without assistance from others.*

We do not understand how a voter can mark, verify or cast a "cast vote record" given the definition of a cast vote record. We suggest deleting the reference to cast vote record.

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots, ~~contest options, and contest selections and vote selections~~ are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by ~~the widest range of all~~ voters.

For clarity and consistency with the Glossary, we suggest some changes to Principle 7: Note that "vote selections" is not defined in the Glossary, but "contest options and "contest selections" are.

- 7.1 - *The ballot design and any default voting system settings for displaying the ballot work for the widest range of voters, and voters can adjust settings and preferences to meet their needs.*

We suggest that 7.1 be changed to make sure that the ballot design on paper also works for the widest range of voters. The original wording assumed that all voters would use an electronic interface. This revision broadens the guideline to include usability of ballots, whether marked with pen or onscreen.

- 7.2 - *Voters and election workers can use all controls accurately, and voters have direct control of all changes of ballot selections~~ballot changes~~.*

- 7.3 - *Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.*

- 7.4 Voters can independently verify the contest selections on the paper ballot before it is cast.

To support "and verified by the widest range of voters before ballots are cast" there should be a guideline that ensures that voters with disabilities are provided a means to verify

independently that what is printed on the paper record agrees with their selections. On-screen (or audio) verification before the paper record has been printed is not sufficient, because the system could print something else on the paper record, as a result of bugs, misconfiguration, or hacking.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE (no comments)

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1 - *An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.*

9.2 - *The voting system produces readily available records that provide the ability to check the correctness of the voting system's tabulation whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.*

The scope of the VVSG does not include eligibility checking. An audit of the voting system cannot be expected to check the outcome of the election without addressing eligibility.

9.3 - *The voting system records are durable, resilient and designed to detect and report exceptions in the presence of intentional forms of tampering and accidental errors.*

9.4 - *The voting system supports efficient audits.*

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters' ballot selections.

We strongly support this principle and its guidelines.

"The secret ballot reduces the threat of coercion, vote buying and selling, and tampering.

For individual voters, it provides the ability to exercise their right to vote without intimidation or retaliation. The secret ballot is a cornerstone of modern democracies."

<http://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf>

The Glossary defines the term "Recallable Ballot" as "Recorded ballot that can be individually retrieved and included or excluded from further processing." We believe that no ballot should be recallable because to do so requires associating the ballot to its voter in the system and violates ballot secrecy. No ballot may be associated with its voter once it has been recorded.

10.1 - *Ballot secrecy is maintained throughout the voting process.*

The definition of "voting process" in the glossary is: "Entire array of procedures, people, resources, equipment, and locations associated with conducting elections." So this

guideline properly assures ballot secrecy during voting, tabulation and auditing of elections.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Principle 11: ACCESS CONTROL (no comments)

Principle 12: PHYSICAL SECURITY (no comments)

Principle 13: DATA PROTECTION (no comments)

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide redundancy against security failures or vulnerabilities.

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

14.2B The voting system does not use wireless technology or connect to any public telecommunications infrastructure.

We recognize that system integrity requires separation from public and all wireless networks. The most prevalent use of networking is for quick results reporting, but there are other means for quickly reporting election results which do not introduce the enormous risks of having a network path back into the voting system.

14.3 - The voting system maintains, verifies and facilitates independent human verification of the integrity of software, firmware, and other critical components.

We also understand that the voting system cannot entirely verify its own integrity and requires human oversight, motivating the above addition.

14.4 - Software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING (no comments)

Suggested Revisions to the Glossary

NOTE: Our Glossary comments here are limited to those relevant to the Principles and Guidelines. We intend at a later date to produce separate comments about the Glossary (and Requirements) that we believe are important. Those are not represented here.

ballot secrecy (This definition should be added to the Glossary.)

No vote can be associated with the voter. The ballot is anonymous. "Voter privacy" addresses the circumstances prior to casting a ballot. In contrast, ballot secrecy refers to the property that is maintained even after the ballot is cast.

ballot selections (This definition should be added to the Glossary.)

Selections made on the ballot by a voter with respect to each contest. Also known as contest selections.

There are numerous instances of usage of “ballot selections” in the draft.

recallable ballot (This definition should be deleted from the Glossary.)

Recorded ballot that can be individually retrieved and included or excluded from further processing.

The concept of a recallable ballot is adverse to the essential principle of ballot secrecy. It does not deserve usage in the VVSG or recognition in the glossary.

cast vote record

Archival tabulateable record of a set or subset of contest selections all votes produced by a single voter as interpreted by the voting system from a given ballot. Also known as CVR. One or more separate cast vote records are generally produced for each ballot sheet.

At minimum there needs to be recognition that a voter may be required to submit more than one sheet and that a cast vote record will represent all or a portion of one or more sheets. ~~each sheet would be at least one separate cast vote record.~~

resilience (This definition should be added to the Glossary.)

The ability to recover gracefully from error conditions and unexpected circumstances. For example, manually marked paper preserves evidence of exceptions that can advise both adjudication and audit to achieve better interpretation of original voter intent.