Open Source Election Technology Institute
530 Lytton Avenue
2nd Floor
Palo Alto, CA 94301 USA
+1 650.600.1450

OSET INSTITUTE

TRUST THE VOTE PROJECT

Tuesday, 09.April 2019

Hon. Christy McCormick
Chairwoman
Hon. Benjamin W. Hovland
Vice Chair

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

RE: Submission of Public Testimony Regarding Voluntary Voting System Guidelines 2.0 to U.S. Election Assistance Commission Hearing, Wednesday, 10th April 2019

May it please Chairwoman McCormick & Vice Chair Hovland

My name is Edward P. Perez, and I have been authorized by our Board of Directors to respond to your invitation and prepare written and oral testimony on behalf of the OSET Institute, Inc.—a 501(c)(3) nonprofit election technology research organization headquartered in Palo Alto, CA with over a decade of experience at the intersection of election system design and cyber-security.

I, together with review by our Chief Legal Officer, also undersigned on this transmittal letter, offer this testimony to the U.S. Election Assistance Commission for reference in its information gathering process regarding pending version 2.0 of the Voluntary Voting System Guidelines (VVSG). We have made every effort to ensure that I, Edward Perez, provide accurate information to the best of my knowledge and experience.

We appreciate the invitation to submit this testimony and my opportunity to appear. We hope this will help inform the Commission's work.

Respectfully Submitted,

Edward Perez
Global Director
Technology Development

Christine M. Santoro, Esq.
Chief Legal Officer &
Corporate Secretary

Before the
U.S. ELECTION ASSISTANCE COMMISSION

In the Matter of	)	PUBLIC HEARING
	)	
VOLUNTARY VOTING SYSTEM	)	Wednesday, April 10th, 2019
	)	
GUIDELINES VERSION 2.0	)	1:00 PM CDT
	)	
DEVELOPMENT	)	Peabody Hotel, Memphis, TN

PUBLIC TESTIMONY SUBMISSION

OSET INSTITUTE STATEMENT BY GLOBAL DIRECTOR OF TECHNOLOGY EDWARD P. PEREZ
REGARDING
THE DEVELOPMENT OF VOLUNTARY VOTING SYSTEM GUIDELINES VERSION 2.0

Introduction

Chairwoman McCormick, Vice Chair Hovland, Commissioner Hicks, Commissioner Palmer, and members of the Election Assistance Commission, thank you for the opportunity to testify about the important matter of the *Voluntary Voting System Guidelines*, Version 2.0. The EAC plays an essential and valuable role in guiding uniform federal standards to support secure, efficient, and accessible elections. The nation owes the EAC a debt of gratitude for all that you do.

My name is Edward Perez, and I am the Global Director of Technology Development for the OSET Institute. I have been authorized by my Board of Directors to prepare this testimony on our behalf. Founded in 2006 in Silicon Valley, the OSET Institute is a 501(c)(3) non-profit, non-partisan organization devoted to election technology research, development and education. The Institute is philanthropically supported, without any partisan or commercial agenda. Our mission is to produce publicly available election technology innovations to increase confidence in elections and their outcomes. Before joining the OSET Institute last year, I worked in the commercial voting system industry for 15 years. As the Director of Product Management for one of the three major vendors, I led a team responsible for writing requirements and achieving certification of a new voting system platform. During my tenure, that platform achieved EAC certification four times, first as a new system, and then through several modification campaigns.

Accordingly, I have no doubt that the promise of VVSG 2.0 represents a pivotal point in ensuring high-confidence elections in a rapidly changing global environment. In the nearly two decades since the inception of the Help America Vote Act (HAVA) and the creation of the EAC, the global technology environment has changed significantly and the greater elections community has had ample opportunity to observe the operation of the federal certification program along with the impacts on the flow of election technology to the nation's election officials. The EAC and the VVSG are well positioned to evolve further and to enhance the effectiveness of the federal certification program.

Today, I focus on three topics that the OSET Institute determined to be critical to the assurance that the VVSG 2.0 is a success in the facilitation of critical innovations for high-confidence elections:

1. Ongoing flexibility in our understanding of the term "voting system;"
2. Component-level certification and common data standards, to support interoperability; and
3. Enhanced agility in the federal certification process, to meet rapidly changing cybersecurity threats.

The OSET Institute (OSET) believes that ongoing re-assessment of foundational issues like these three, consistent with HAVA, can be addressed at the program management level (e.g. updated manuals for *Testing and Certification* and for *Voting System Test Laboratories*). Furthermore, the application of VVSG 2.0 to the realities of the environment as it exists today is essential for success. This can be measured by the continuous delivery of innovative election technology in a competitive, diverse marketplace that is responsive to the needs of election administrators, voters, and the vital national security needs of the nation as a whole.

1. Definition of "Voting System"

The Help America Vote Act adopted a broad definition of "voting system" for legislative purposes, encompassing a wide scope of components, functions, practices, and documentation in its description of the term. Notwithstanding typical practices from major voting system vendors and testing authorities in recent decades, OSET believes that the EAC has an opportunity to consider the scope of "systems" and "components" to which the VVSG 2.0 requirements apply in a more flexible and nuanced way. More specifically, OSET 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 thinking of a "voting system" in a manner still consistent with HAVA's definition.

Having worked in the commercial voting technology industry for many years, it is my professional opinion that few things have been more consequential for innovation and choice, or the lack thereof, than a "total-sum" concept 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 fit within 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 well-intentioned, has ironically resulted in a highly-concentrated marketplace that reduces competition, increases dependence on vendors, and leaves our nation's elections officials with fewer choices.

The voting technology industry has become concentrated to the point where the two largest providers supply voting systems for approximately 80% of the nation's registered voters. The fact is, only *one* new vendor has meaningfully entered the marketplace in the past decade, which dramatically illustrates how complexity can produce inertia. The total-sum concept 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.

It is my professional opinion that voting system manufacturers perceive a greater return on investment in making functional changes to their systems mainly, or even exclusively, to open new regional markets, rather than addressing the ongoing needs of current customers through value-added enhancements. 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."

2. Component-Level Certification, Common Data Formats and Interoperability

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," OSET means 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, EAC certification could thereby "raise the bar" for the overall state of the art, by allowing wider distribution and deployment of technology innovations.

[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.

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 invested into VVSG 2.0 functional requirements, catalyzed by more than a decades' work of engagement and learning by many stakeholders, much of the effort that would otherwise 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.

3. The Cyber-Threat Landscape Requires Agility

The third and final point I want to address is the imperative reason why an evolving understanding of "voting systems," as well as component-level certification, are so valuable and indeed essential. Our national security depends on the agility that these programmatic changes can help to deliver. The cyber-threat landscape is rapidly changing. For example, Zero-Day Vulnerabilities[2] are an increasing occurrence. Therefore, in the future, it will be imperative that the VVSG 2.0 federal certification program support rapid changes to voting technology, at a pace faster than the last two decades have experienced.

[2] A zero-day vulnerability is a basic flaw in design and/or implementation of hardware and/or software. It is an unknown exploit that exposes weakness and can create problems long before it is realized something is wrong. There are many reasons for zero-day exploits from hasty development to lack of security-centric engineering practices. A zero-day exploit leaves no opportunity for detection initially. A zero-day attack occurs once that flaw is exploited and attackers release malware before an opportunity to create a patch to fix—thus, it is "zero-day(s)" in occurrence. OSET believes it is important to understand the zero-day exploit timeframe and consider—in lack of digital security standards and guidelines—how that can easily become a challenge for voting systems.

- A company's developers create software, but unbeknownst to them it contains a flaw.
- The attacker spots that vulnerability either before the company does, or acts on it before the company has a chance to remedy the flaw.
- The attacker writes and implements code to exploit the flaw while the vulnerability is still undetected.
- After releasing the exploit, either the public recognizes it in the form of a system compromise, or the company (hopefully) catches it and creates a patch to stop the potential consequences.

Once a patch is written and applied, the exploit is no longer called a "zero-day exploit." These attacks are rarely discovered right away. In fact, it often takes not just days but months and sometimes years before a company learns of the vulnerability that can or did lead to an attack. This is one of the reasons the OSET Institute is so bullish on code transparency, peer-review, and extensive vetting.

Our nation's adversaries are not standing still. As technology advances, so do the cyber-warfare tools with which they seek to undermine our democracy and diminish the public's faith in election outcomes.

The danger that must be avoided is the possibility of simply re-creating the cumbersome scope, complexity, and dependencies that have led to relative inertia in the voting technology marketplace.

If the VVSG 2.0 program only considers voting systems in their totality, as in the past, and if the flexibility of component-level certification is not offered at the federal level, the likelihood is that it will be years before any manufacturer starts to work on a VVSG 2.0-compliant system.

Furthermore, as with all new standards and supporting testing and certification procedures, there is also no guarantee that testing campaigns will proceed efficiently the first time, which could mean further delays before 2.0-compliant technology is available to election officials. Needless to say, by that time, the cyber-threat landscape will almost certainly have moved beyond the threats those products were designed for in the first place.

In contrast, focusing on cybersecurity requirements for individual components is a far more tractable problem that can be worked on much more quickly, with faster results. Focusing on the security requirements for a tabulation sub-system, for example, is far more actionable, for a wider array of security experts, than is the task of creating end-to-end security for an entire system of systems in 2019 or 2020. Cybersecurity experts would not even need to begin with election-specific requirements; those can be added to the state-of-the-art for secure systems more generally. As noted previously, security requirements for individual voting system components could also be drawn from the current work that has already been done with VVSG 2.0, and those requirements can continue to evolve over time, if they are created in a more targeted manner.

In Closing

In conclusion, the OSET Institute believes that the recommendations described in this testimony can greatly help the EAC to further the goal of protecting election infrastructure as a matter of national security.

We believe that any attempt to compromise that infrastructure, or the administration of elections, or any of the processes of free and fair elections as a part of the operational continuity of our democracy at any level of government, is a violation of our nation's sovereignty.

Going forward, we further believe that the VVSG 2.0 and the EAC federal certification program must support agile updates and upgrades to our electoral infrastructure to afford it the verifiability, accuracy, security and transparency essential to free and fair elections where ballots are counted as cast, and confidence is high in elections and their outcomes.

To this end, we appreciate the EAC's leadership in ensuring the security, accessibility and sustainability of voting technology.

Respectfully Submitted,

Edward P. Perez

Global Director, Technology Development
OSET Institute, Inc.
Palo Alto, CA

Tuesday, 09th April, 2019 13:30 PDT

Resources in Support of Testimony

OSET Critical Democracy Infrastructure Briefing:
http://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure

National Security Threats to Election Infrastructure:
https://trustthevote.org/wp-content/uploads/2018/02/oset_protectingelectiontech_nov7.pdf

Appropriate Use of Open Source Technology in Government Mission Critical Computing:
http://www.osetfoundation.org/research/2018/3/12/appropriate-use-oss