OSET INSTITUTE

Position Paper

Version 4.2

Rethinking Election Technology Certification

New Cybersecurity Threats Require New Thinking on Testing and Certification

Prepared for:
U.S. Election Administration & Public Policy Leadership

Prepared By:

Edward Perez
Global Director, Technology Development

Contributions From:

Gregory Miller
Co-Founder, Chief Operating Officer

May 2019

Context

When the Help America Vote Act was passed in 2002 and the regulations implementing the U.S. Election Assistance Commission (EAC) and provisions for testing and certification were put in place, little thought was given to the sources and methods of potential "attacks" on the sovereign act of free and fair elections. Indeed, we argue that the focus 15 years ago was primarily on clearly ascertaining and protecting voter intent. At the time, the thinking was that computers can easily and reliably do that. No one was thinking about "digital attack vectors" on what would be the new machinery of election administration and voting. In some ways similar to other historical mindset-changing events (e.g., the Pentagon Papers, Watergate, the 9.11 attacks, etc.), there remained an "age of innocence" with regard to the integrity and security of computers in voting.

Of course, that innocence was somewhat ironic. Even in 2005 computer viruses and malware were well-understood threats. Nevertheless, this administrative computing segment, severely lagging behind the majority of Government I.T., has a growing blind spot. Inasmuch as the election of 2000 woke a nation to the vulnerabilities in our processes of voting, the election of 2016 woke a nation to the reality that the very thing intended to lead us away from the problems of the "hanging chad" had brought us to a new reality: the impact of having never applied proper threat models, risk assessments, or security-centric engineering in the design, development, testing, and certification of the machinery upon which now we depend for the defense of our democracy. It is past time to rethink testing and certification. The OSET Institute takes a position on that topic in this Paper led by our Global Director of Technology Development, Eddie Perez.

1. The Expanding Scope of Election Security – Voter Registration and Network-Connected Systems

On an almost daily basis, there is mounting evidence that the scope of “election security” is wider than might appear at first blush. While much attention has been paid to “voting machines” and “voting systems”[1] that capture and tabulate votes, there is growing awareness that other types of election-related software infrastructure are even more vulnerable than (*usually*) air-gapped voting systems, by virtue of being network-connected: specifically, voter registration (VR) systems and Election Night Reporting (ENR) systems (which display results over the web, but which do *not* tabulate votes) have been found to be especially vulnerable.

The recently-released Mueller Report determined that the Russian GRU infiltrated the Illinois State Board of Elections[2] web site in June/July 2016 and reviewed approximately 80,000 voter registration records; the Federal Bureau of Investigation (FBI) also confirmed that Russia penetrated the IT network of “*two Florida Counties*.”[3] And finally, in March, the Department of Homeland Security (DHS) and the FBI issued a Joint Intelligence Bulletin (JIB)[4] to state and local authorities, which confirmed that that the Russian reconnaissance and hacking efforts in advance of the 2016 election went well beyond the 21 states confirmed in previous reports. According to the bulletin, "*The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US states’ election networks leading up to the 2016 Presidential elections* [emphasis added]." Needless to say, whether such attacks are actually successful or not in compromising the integrity of voter registration records, even the possibility that one’s eligibility to vote could be thwarted by a corrupt actor can undermine public faith in the legitimacy of election outcomes.

2. Early Federal Steps Toward A Broader View on Cybersecurity

In light of cyber-attacks like these, as the nation bolsters its cybersecurity defenses, new standards and security procedures will be necessary for a variety of network-connected election systems, including voter registration, election night reporting, and e-poll book systems, as these currently fall outside the scope of the federal certification program for voting systems (i.e., the U.S. Election Assistance Commission’s testing for compliance with the *Voluntary Voting System Guidelines*).

[1] Even air-gapped machinery is vulnerable when one considers the insidious nature of physical delivery vectors such as USB sticks (think: STUXNET). Nonetheless, network connectivity for systems serving other aspects of election administration (and **not** ballot casting or counting) can pose a serious risk, and those systems using such capabilities require considerable (and regular) pen-testing.

[2] https://chicago.suntimes.com/news/mueller-report-special-counsel-russia-hacking-illinois-state-board-elections/

[3] https://www.politico.com/states/florida/story/2019/05/14/russians-accessed-voter-records-in-two-florida-counties-fbi-confirms-1015760

[4] https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/

Thankfully, the importance of expanding the nation's cybersecurity focus beyond voting systems has reached the halls of Congress. For example, Senator Ron Wyden's (D-OR) "*Protecting American Votes and Elections Act of 2019*" (PAVE)[5] is a strong, comprehensive, and pragmatic election security bill recently introduced in Congress. Notably, in addition to requiring durable paper ballots and risk-limiting audits for federal elections, the PAVE Act recognizes the changing landscape by envisioning a new cybersecurity testing role for DHS — and its requirements encompass not only voting systems, but also Voter Registration systems, Election Night Reporting, and Digital (electronic) Poll Books.

As the PAVE Act illustrates, recognizing the wider scope of the cyber-threat landscape is undoubtedly a critical first step, and is laudable. After that first step, however, things start to get complicated, quickly. Why? Because deciding "*what*" we need to protect is almost certainly easier than figuring out "*how*" to devise federal institutions and programs that can perform effective testing and certification of technologies that have not previously been addressed under current federal certification programs.

3. OSET Institute Advice: Sweat the Details, Because Process is All-Important

In light of these recent efforts to "do more" and "protect more," the OSET Institute's message to legislators is a modest one:

> *Proceed cautiously, and do not assume that simply "parceling things out" between DHS and the EAC will be easy or straightforward.*

If there's one thing that we've learned since the Help America Vote Act (HAVA) was enacted in 2002, thereby creating the Election Assistance Commission (EAC), it's this: creating federal standards (*for any kind of technology*) is only the first step; the unique institutional implementation of testing and certification programs is at least as impactful— if not *more* impactful —than the standards themselves. Again, "*how*" can be more consequential than "*what*." For example, despite the fact that the EAC adopted updated voting system standards (VVSG 1.1) in 2015, no voting system manufacturer has submitted a system for testing to anything other than the 14-year old VVSG 1.0 standard. Despite the fact that those 2005 requirements are not adequate for the current global environment, or for current voter needs, the manner in which the EAC implemented the federal VVSG certification program for "new" and "modified" voting systems allows vendor practices that lead to troubling, sub-optimal outcomes. The devil is in the details.

For the same reasons, any efforts to expand federal testing and certification programs should also be considered evolutionary – in other words, different technologies and different requirements will likely require programs very different from the ones we are familiar with today. While it is perhaps natural for legislators to think, "*give this task to the EAC*," or "*give this task to DHS*," and then simply assume that new needs can be assimilated to current procedures, the OSET Institute recommends that new programs be devised thoughtfully and methodically, with fresh eyes.

[5] https://www.wyden.senate.gov/download/protecting-american-votes-and-elections-act-of-2019-bill-text

Today's EAC program and EAC resources are almost certainly not adequate or appropriate for cybersecurity testing of network-connected systems like VR systems, ENR systems, and electronic poll books. These technologies have an operating environment that is very different from voting systems, with different technical requirements, and the EAC has relatively limited experience with them. Conversely, while DHS has core competencies and resources devoted to cybersecurity for high-assurance systems (in a way that the EAC and current EAC-accredited Voting System Test Laboratories (VSTLs) do not), DHS's institutional capacities and domain knowledge associated specifically with elections are currently more modest, by virtue of becoming significantly active in this sector only recently (i.e., since 2016). We note that the EAC's recent acquisitions of professionals with election administration experience and talents bode well for this to evolve.

For all of these reasons, the OSET Institute believes that an approach that simply amends HAVA, preserving many of the testing and program assumptions applicable to voting systems, and "adding on" new requirements for the EAC and DHS to address cybersecurity vulnerabilities in new types of election-related technologies are likely to exacerbate shortcomings in the current program. This is especially true in light of recent Congressional oversight hearings in which the EAC described the paltry state of its approximately $8.5 million operating budget (after transfers of $1.5 million to the National Institute of Standards and Technology), which has no signs of being significantly increased in the near future.[6]

In addition, adding a new layer of complexity and potential friction to current practices will pose new challenges for voting system manufacturers and election officials alike, as they will be required to traverse two sets of potentially overlapping, redundant, or conflicting requirements. The election technology marketplace has already been distorted by the cost and complexity of one federal election technology certification program; simply adding more on top of it (or in competition with it) could make those unintended consequences even worse.

Despite the fact that current EAC and DHS programs provide no easy roadmap for the expansion of cybersecurity standards for VR systems and other network-connected elections-related software, the Help America Vote Act (HAVA) can still be a useful model for the kinds of programmatic questions that legislators should focus on to develop new testing and certification programs in the future. Specifically, it is instructive that *all* of HAVA's Title II – a long 32-page section of the Act, with 4 Sub-Titles, constituting approximately *half* of HAVA's total pages – is devoted *solely* to fundamental topics about the EAC's creation, organization, duties, and procedures. This section of HAVA can be a useful model for thinking through the institutional and programmatic aspects of how best to allocate testing and certification responsibilities in the future. Among the important questions HAVA's Title II addresses are:

- How is the testing and certification body established?
- What is its membership, and who is qualified to be a member?
- What are its duties?
- What are its powers?
- Who is responsible for providing technical guidelines and relevant functional requirements?

[6] https://about.bgov.com/news/election-agency-resources-shrink-as-foreign-hacking-threats-rise/

- What is the process by which requirements are adopted?
- What is the process by which requirements can be modified?
- What types of laboratories or third parties are qualified to perform testing and certification?
- How are third-party testing labs accredited?

To be clear: the OSET Institute believes that the changing cyber-threat landscape requires new testing and certification programs that answer the kinds of questions above. And we strongly caution that the answer to these questions is not simply, "*What HAVA said*," or "*What the EAC said*."

Creating standards for VR systems, Digital Poll Books, and ENR systems, and devising new cybersecurity requirements not just for these but also for voting systems, is new territory. Accordingly, it requires new and different institutional responses, which should be crafted thoughtfully and methodically.

4. Recommendations For Going Forward

The national security imperative to bolster cybersecurity for an expanding scope of election-related infrastructure represents a pivotal point in ensuring high-confidence elections in a rapidly-changing global environment.

In order for election administrators to meet future challenges, states and federal legislators, the EAC, DHS, and other stakeholders must continue to evolve and critically re-assess existing federal certification processes. A major objective is ensuring that high-quality voting technology can be certified at a faster pace, by testing authorities with increasingly specialized qualifications, at reasonable costs that are affordable for large and small jurisdictions alike.

In an April 2019 blog post[7] I expressed the Institute's belief that continued agility and adaptability in protecting election infrastructure depends on a three-part focus:

1. A more flexible definition of "voting system;"
2. Component-level certification; and
3. Support for more rapid changes to election technology, at a pace faster than the last two decades have seen.

One point about that third element: The Institute's position from the beginning has been that innovation of election technology is significantly behind the majority of government I.T. (which is itself often a generation behind commercial I.T) for a variety of market dynamics reasons. However, post 2016 there can be no doubt any longer that election technology must adapt, evolve, and innovate far more rapidly in order to keep pace with what essentially is a digital arms race. For the most part, where network- (or cloud-) enabled services are involved the focus may be more on the configuration and deployment elements, but regardless, protecting election administration technology infrastructure requires the ability for the testing and certification aspects to become more agile and responsive to a shortening cycle time for innovations.

[7] https://www.osetfoundation.org/blog/2019/4/12/perspectives-from-the-us-elections-assistance-commission-public-hearing-in-memphis

Accordingly, the combination of new allowances for component-level EAC certification, in conjunction with DHS oversight of cybersecurity testing (entirely separate from testing for VVSG-compliance) could be a good first step in the right direction.

Compared to the daunting task of creating end-to-end security for an entire system of systems in 2019 or 2020, focusing on cybersecurity requirements for individual components is a far more tractable problem that can be worked on more quickly, with faster results.

Furthermore, the Institute believes that component-level cybersecurity testing will be most effective if paid for by DHS, unlike the current EAC testing program, which can create conflicts of interest because voting system vendors pay the fees of the VSTLs that perform compliance testing.

Consider this: Rather than relying on EAC-accredited VSTLs, which do not have a core competency in high-assurance cybersecurity, DHS could, for example, rely on laboratories accredited by the National Information Assurance Partnership (NIAP),[8] which is a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). In the U.S., NIAP is responsible for implementing the internationally recognized Common Criteria Recognition Arrangement (CCRA),[9] which is a framework by which government, military and other users can specify their security functional and assurance requirements through the use of protection profiles. Vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. This combination of component-level certification and alternative laboratories accredited through NIAP is just one example of how federal certification programs for election-related technologies could evolve.

Whatever form testing and certification programs might take going forward, this much is clear: they need to be planned carefully, and it should not simply be assumed that HAVA, the EAC, or past practices will provide guideposts on the road that lies ahead.

In any event, the tough work of evolving and adapting is just getting started.

[8] https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs/NIAP_NCSC_factsheet.pdf

[9] https://www.commoncriteriaportal.org/ccra/