The Case for Voluntary Certification of Our Entire Election Ecosystem

In an age when election security is one of the most high-profile national issues, voluntary certification across the board not only increases public confidence, it offers tangible benefits to both states and vendors.

Voluntary federal certifications of several key parts of the electoral system are already a part of the landscape and are at least nominally familiar to all of us. Tabulation systems, e-pollbooks and election hardware are commonly federally certified and many states have their own certification processes as well. We believe those voluntary certifications are not just a good thing but one that should be expanded to other areas of the elections ecosystem, including Voter Registration and Election Management software systems.

THE MODEL AND MECHANISMS ARE ALREADY IN PLACE

The federal government and many states already have certification processes in place and are deeply familiar and experienced in the elections workspace. Currently, the U.S. Election Assistance Commission (EAC) provides certifications for tabulation systems and voting hardware. Those certification processes already in place could be utilized as a template, revised, and enriched where needed to also certify Voter Registration and Election Management systems. Once established, states could choose individually whether or not to make federal certification a requirement and also add their own extra requirements if they so choose. The EAC is also piloting a program with the Center for Internet Security to expand election technology verification programs, signaling a need for more consistent evaluation criteria.

ENHANCED SECURITY AT A CRITICAL TIME

Perhaps at no other time in history have the inner workings and mechanics of the election process been more in the spotlight. Simultaneously, cyber criminals and other

nefarious actors have grown in numbers and sophistication, presenting new and ever-changing threats to our elections systems—especially those dependent on sophisticated software—software that often includes critical components or features from third-party vendors.

Given that, robust voluntary certification of all facets of elections systems could greatly increase cybersecurity and resilience, while enhancing voter confidence. One way to do this could be to include in the certification process the standards of the Department of Commerce's National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework helps entities of all sizes better understand, manage, and reduce their cybersecurity risk and protect networks and data.

APPLICATION OF PROVEN SECURITY STANDARDS TO ALL VOTING SYSTEM COMPONENTS

Expanded voluntary certification could also include adherence to the Federal Risk and Authorization Management Program (FedRAMP). This government-wide program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information, and helps accelerate the adoption of secure, cloud solutions. We look to these standards for our clients as well, running our solutions on AWS GovCloud (US) Regions, which are designed to host sensitive data, regulated workloads, and address the most stringent U.S. government security and compliance requirements.

In addition, certification could also utilize penetration testing, including by law enforcement agencies such as the Department of Homeland Security (DHS). Elections system testing could also be conducted by federally or nationally accredited Voting Systems Test Laboratories (VSTL) to ensure all systems meet federal standards.

What's in it for me? Benefits to States

MORE CONFIDENCE, FEWER RESOURCES EXPENDED

Expanding voluntary certification to all voting systems, including Voter Registration and Management systems will provide secretaries of state and citizens an extra layer of confidence in their voting infrastructure, knowing that a knowledgeable and experienced entity has done the review. In addition, rather than each state needing to create its own certification (thereby duplicating work across each state government), states would be freed up to concentrate on other important tasks, especially system performance, knowing that vendor software products have met the uniform federal certification standards for security.

PUTTING SECURITY CONCERNS IN A SAFER PLACE

Procurement processes would be greatly streamlined and quicker given states would no longer have to spend large amounts of time on independent deep security reviews. Security certifications would now be in the hands of truly experienced and specialized subject matter experts. Relying on voluntary federal certification would also insulate state offices from IT staff turnover and the resulting losses of institutional knowledge such turnover invariably brings.

ELEVATING QUALIFIED VENDORS

Consistent and uniform federal standards of certification would also quickly expose those vendors whose products and performance are lacking – issues that are often-times difficult to spot during a typical procurement process. This would help states more readily identify poor performers, saving time and vetting efforts. This transparency would also apply to constituents, who would now be able to readily identify if election systems are certified.

> **Moreover, at the end of the day, secretaries of state will be able to point to tangible evidence – the federal certification – to show that they've done their due diligence and taken all the steps possible to maintain a secure and properly vetted system, including all its components.**

What's in it for me? Benefits to Vendors

IT'S NOT JUST YOU SAYING YOUR PRODUCTS ARE SECURE

People today are very accustomed to being able to readily verify product claims and service standards via third-party reviews. By the same token, vendors should welcome an independent voice saying their product is up to or exceeding standards and providing an extra layer of confidence that their products are a secure and trustworthy part of the election process.

Utilizing federal standards provides uniform benchmarks for certification - and decertification when appropriate. The testing done via accredited independent labs would also assist vendors in staying up to date in security matters and keep a step ahead of the constantly evolving and ever more sophisticated threats.

ANOTHER PRODUCT BENEFIT FOR VENDORS TO TOUT

Being able to say their systems adhere to and or exceed national standards is a provable, black and white selling point and one that is likely to place vendors on the short lists for state RFPs. And again, since it's coming from a third-party source of truth, potential customers are far more likely to place value in certified products than those that are not.

A NEW TRANSPARENCY FOR VENDORS ON POTENTIAL THREATS

Vendor systems almost always rely on third-party software products that may have unknown vulnerabilities or security concerns—at least they're generally unknown until there's a major problem. Applying federal standards to all components of the elections ecosystem would ensure vendors that when vulnerabilities or critical errors are found in a third-party software, all certified vendors using it will be informed and able take action to remedy the problem. As it stands now, bad actors can find a weakness in a third-party software, exploit it, and then simply repeat the same attack with other systems using the same third-party software.

Properly implemented, voluntary standardized certifications could prevent a repeat of scandals, such as the recent incident whereby election workers' personal data were transferred to China instead of remaining in the U.S. as required.

THE TIME TO ACT IS YESTERDAY

Certainly, there are many stakeholders from various backgrounds and perspectives but perhaps the one thing they can all agree on is the critical need to maintain, improve, and secure the health of the entire elections ecosystem. And just as your doctor checks and verifies your overall well-being—not just a part of your body—so too should we implement the steps necessary to ensure every part of our election systems are healthy and able to fight off the threats that attack every day. It's not just a win/win for all involved, it's an essential investment in the health of our democracy.

CIVIX

Recognized as one of the top government software and service providers in the U.S., Civix is on a mission to transform the public sector.

Learn more:

GoCivix.com

Contact us:

Solutions@GoCivix.com

1-888-GOC1V1X