Partnerships and Independent Research Offer New Protection for Elections

ES&S ELECTION Systems & Software

When it comes to the security of election technology, the threat landscape is constantly shifting. That's why it's vital that the efforts to secure and maintain the security of elections continue to evolve and expand.

Voting system manufacturers must look to the future to face challenges head-on and to prepare for the unknown.

Involving resources and creating partnerships across and outside the election community can help ensure the security, accuracy and accessibility of modern voting technology.

Critical Infrastructure Benefits from Partnerships

The election landscape of today is far from where it was just a decade ago. Fueled by a growing concern among American voters regarding election integrity and a desire to instill trust in election systems, voting system manufacturers began to rely on new partnerships and tools to bolster the security of voting systems — particularly after the 2016 election. In 2016, the emergence of nation-state threats to American election infrastructure resulted in demand for more and better security testing.

In 2017, when elections were included as critical infrastructure under the U.S. Department of Homeland Security (DHS), election officials and suppliers were afforded access to expanded federal resources to harden systems against physical and cyber threats. In conjunction with the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigations (FBI), the Center for Internet Security (CIS) and the U.S. Election Assistance Commission (EAC), voting system manufacturers became ingrained in organizations such as the Sector Coordinating Council (SCC), Multi-State Information Sharing and Analysis Center (MS-ISAC), Election Infrastructure ISAC (EI-ISAC), Information Technology ISAC (IT-ISAC) and the subset Elections Industry Special Interest Group (EI-SIG) – a cybersecurity information-sharing group for election industry providers to guard their networks and assets against threats. This access and collective approach meant the industry could make greater strides in continuous improvement to election security.

The knowledge gained from these partnerships led to greater collaboration and threat sharing with both federal agencies and the cybersecurity community. For the first time,

The knowledge gained from these partnerships led to greater collaboration and threat sharing with both federal agencies and the cybersecurity community.

DHS included election officials and election technology manufacturers in the Private Sector Clearance Program, giving them security clearances and access to classified briefings about threats to elections. Critical elections infrastructure suppliers also began taking part in Critical Product Evaluation (CPE) testing programs and seeking out the expertise of other independent cybersecurity researchers, such as those at private companies and academic institutions.

Today, voting system manufacturers regularly place voting systems in the hands of independent researchers, putting vital election technology through the paces of pervasive penetration testing of hardware and software using the same modern security tools hackers use. This helps to ensure equipment is secure before it ever reaches a jurisdiction.

Coordinated Vulnerability Disclosure as a Standard Practice

One independent research method for election infrastructure is made possible through the principles of coordinated vulnerability disclosure (CVD). CVD policies set the rules of engagement for an ethical hacker to identify and submit information on security vulnerabilities, establishing a framework for voting system manufacturers and researchers to formally exchange information on any potential security weaknesses or vulnerabilities. While CVD programs are relatively new to the elections industry, CVD programs are frequently used by other industries (airline, automotive, healthcare, for example) as a productive and beneficial way for independent researchers to help improve the security of networks, systems or applications.

CVD policies set the rules of engagement for an ethical hacker to identify and submit information on security vulnerabilities.

A CVD program involves a number of key components, including a clear set of guidelines for the rules of engagement, a process for reporting, a commitment to act in good faith with the researcher and follow through with any potential remediation or mitigation and disclosure. The elections industry built a CVD framework and policies in collaboration with CISA based on best practices established by numerous other private sector industries.

Pilot Event Builds Bridges

In September 2023, several of America's leading voting equipment manufacturers collectively opened their latest voting equipment to a new type of in-depth scrutiny by some of the best independent cybersecurity researchers in the U.S. The first event of this kind, the Election Security Research Forum, aimed to further the security and transparency of elections.

Over a dozen trusted security researchers were given access to the types of new election technology voters may encounter at a polling site in the future. Under the principles of CVD, researchers had unprecedented access to test digital scanners, ballot marking devices and electronic pollbooks. All the software configurations tested at the Forum were newly developed and not yet fielded at the time of testing.

The Forum was organized through the Information Technology – Information Sharing and Analysis Center (IT-ISAC) and included three leading voting equipment manufacturers. An independent advisory board comprised of security researchers, security companies, nonprofits and former state and local election officials selected the security researchers involved in the event.

Feedback received following the Forum was overwhelmingly positive from researchers and technology providers.

Feedback received following the Forum was overwhelmingly positive from researchers and technology providers. The event fostered and strengthened relationships between the security and supplier communities and will ultimately bolster the security and resilience of voting technology. Researcher findings at the event were shared with manufacturer participants, who will address findings under their coordinated vulnerability disclosure programs.

Opportunities Abound with Independent Research

While voting system manufacturers have engaged in independent security testing for many years through voluntary testing programs, the pursuit of improved security is never-ending. Further work with trusted independent security researchers provides opportunities to improve the security and transparency of tomorrow's voting technology.

1. **A new point of view.** The security-minded people inside internal manufacturer product teams are very good at what they do, but the same set of eyes looking at the development of software and hardware can narrow the point of view. Having independent researchers test the security of equipment from a new perspective can help internal developers produce stronger, more resilient products with a broader range of threat defenses.
2. **Meeting threat evolution.** Election security is an ongoing process. Independent research can contribute to continuously monitoring systems and processes, ensuring they evolve to counter new threats. Encouraging collaboration between researchers, government agencies, academic institutions and technology companies can facilitate information sharing, leading to a better understanding of threats and more effective security measures.
3. **Testing transparency.** Working with independent researchers and producing a collaborative report that addresses CVD is a productive, structured way to share information about the testing of election technology, unlike independent testing program reports that may contain proprietary and confidential information about voting systems and aren't released publicly to avoid giving hackers a roadmap of critical infrastructure. Research conducted under CVD can produce public reports, allowing for a transparent process that reassures voters of the strength of voting systems.
4. **Greater success at formal testing.** As part of the federal formal voluntary testing program, the U.S. Election Assistance Commission (EAC) recently launched a penetration testing program. Informal testing events with independent researchers help manufacturers create stronger systems and better internal testing programs, allowing for greater success when submitting a new system for certification to the EAC and their new security testing program.
5. **More secure elections.** Ultimately, increased testing and greater transparency lead to more secure elections and greater confidence that the systems fielded for local elections are secure, accurate and accessible.

Providing Election Experts Increased Confidence

Local and state officials who administer elections are the undisputed election experts. But that doesn't always mean they are security experts regarding the technology or equipment used in elections.

In the same way that manufacturers partner with election administrators to ensure that systems are usable and meet the needs of voters, working with independent researchers is just one additional way voting system manufacturers help provide administrators with increased confidence in their systems — knowing they are tested, proven and trusted.

Overall, independent research acts as a critical watchdog, identifying weaknesses, proposing solutions and ultimately bolstering the security and trustworthiness of election systems.

Learn more about the Election Security Research Forum pilot program here:
https://www.essvote.com/blog/industry-news/pilot-program-aims-to-further-the-security-and-transparency-of-elections/

ELECTION Systems & Software

About ES&S

Election Systems & Software (ES&S) is the nation's leading voting systems manufacturer. For more than 40 years, ES&S has been supporting elections by creating and providing secure, accurate and accessible voting equipment to jurisdictions across the country. Learn more about ES&S at www.essvote.com and on Facebook at facebook.com/essvote.