Election Security
Research Forum
Presented by IT ISAC

Frequently Asked Questions (FAQs)

September 2023

What is the purpose of the Election Security Research Forum?

This pilot event aims to help shape a clear and concerted approach to establishing processes by which security researchers and U.S. election technology providers can work together under principles of coordinated vulnerability disclosure (CVD) to enhance the security of elections technology and increase overall confidence in U.S. elections.

Who is leading the Election Security Forum?

The Election Security Research Forum is organized through the Information Technology – Information Sharing and Analysis Center (IT-ISAC), a nonprofit organization comprised of technology companies that have organized to enhance their cybersecurity posture, and the security of critical infrastructure, by sharing threat intelligence and best practices to mitigate threats.

The forum is being facilitated by the IT-ISAC's Elections Industry Special Interest Group (EI-SIG) and organized with the assistance of an independent advisory board comprised of security researchers, security companies, nonprofits, and former state and local election officials.

Advisory Board members include:

- Jared Dearing, Center for Internet Security
- Casey John Ellis, Co-Founder and CTO, Bugcrowd
- Matthew Masterson, Microsoft
- Chloé Messdaghi, Head of Threat Research at Protect AI
- Jennifer Morrell, CEO & Co-Founder, The Elections Group
- Alex Rice, Co-Founder and CTO, HackerOne
- Michael A. Specter, Security Researcher
- Trevor Timmons, Chief Technology Officer, The Elections Group

Grant funding to cover travel costs for participating researchers is being provided by the Center for Internet Security (CIS), a nonprofit that harnesses the global IT community to safeguard public and private organizations against cyber threats.

Why is MITRE hosting the Election Security Research Forum?

As an independent and trusted adviser to government, industry, and academia, MITRE connects these groups to convene and discuss how to pioneer for the public good and solve problems that challenge our nation's stability. The Election Security Research Forum organized by the IT-ISAC furthers research to pioneer new election technology, aligning with MITRE's mission.

For 65 years, MITRE has helped the nation's most critical organizations mitigate risk through analysis and objective insight, free from commercial interest. MITRE is a unique national resource in risk analysis, with decades of innovation and experience partnering with government and industry to understand and mitigate risks related to the country's national and economic security, and critical infrastructure.

MITRE's National Election Security Lab (NESL) conducts comprehensive and objective security testing and vulnerability analysis on the entire election ecosystem, subsets of the ecosystem, or individual components. NESL provides election officials, vendors, the Department of Homeland Security, the U.S. Election Assistance Commission, and other key stakeholders, a trustworthy, secure, representative, reconfigurable environment in which to place their actual IT and election equipment and software to safely develop risk management options.

Who is taking part in the Election Security Forum?

Three members of the IT-ISAC Elections Industry Special Interest Group volunteered to participate in this unique opportunity to test a remarkably wide swath of modern technology that will be fielded in the future across the U.S: Election Systems & Software (ES&S), Hart InterCivic, and Unisyn Voting Solutions. Combined, these companies supply election systems for a significant number of election jurisdictions across the nation.

What equipment will be included?

With three diverse companies participating in the event, researchers are receiving access to a variety of election technology. Each company is responsible for determining the hardware they make available for the event. This robust offering collectively includes digital scanners, ballot marking devices, and electronic pollbooks with a primary focus on the technology that voters may encounter at a polling site.

- Across all the participating companies, the configuration of the resident software being tested at the pilot forum has yet to be deployed in a live election.
- Some hardware being presented at the forum may already be in use, while other hardware has yet to be introduced into the market. This varies by company.

How were the researchers selected?

Researchers were selected by the independent advisory board based on the researchers' technical experience and commitment to engaging under the principles of Coordinated Vulnerability Disclosure. The advisory board includes companies that regularly engage with highly proficient security researchers.

How does this event differ from other kinds of voting system testing?

Registered U.S. manufacturers of certified election systems already engage in robust testing and certification of their products, including adversarial penetration testing. For this pilot event, participating companies are voluntarily making their systems available for third-party review as part of a standard company coordinated vulnerability disclosure (CVD) process, where individuals may report potential security vulnerabilities to the manufacturer for consideration. Researchers taking part in the forum have agreed to follow the companies' coordinated vulnerability disclosure (CVD) policies, including timelines for independent disclosure of their research for the systems with which they engage.

What is a vulnerability?

According to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), security vulnerabilities are "common attributes of a hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."[1] In general, vulnerabilities can arise due to software bugs, misconfigurations, insecure design, or user errors.

How will discovered vulnerabilities be addressed?

Manufacturers will collaborate directly with the researchers to evaluate whether any finding would impact the proper operation of the technology. In addition, the manufacturer and researchers will consider if any existing compensating controls are in place to reduce or eliminate the risk or the severity of a validated vulnerability and include this information in any report of the vulnerability.

What should jurisdictions do if a vulnerability is discovered on a piece of hardware they currently use?

The configuration of the resident software present on the units being tested at the pilot event is newly developed and not yet fielded. However, should election officials have questions about any research findings, they should contact their voting system manufacturer directly for further information and next steps.

[1] CISA, "Guide to Vulnerability Reporting for America's Election Administrators," (July 2020), available at https://www.cisa.gov/sites/default/files/publications/guide-vulnerability-reporting-americas-election-admins_508.pdf.

Why should voters trust equipment that has a known vulnerability?

Voters can trust the equipment they use to cast ballots because of the robust and accountable design of the underlying election process. The accountability, transparency, and audit functions in the underlying election process are designed to mitigate the impact of any individual vulnerability. Efforts like this event with security researchers go a step further to add transparency to the process, with the goal of educating the public, broadening accountability, and engendering trust. It is also important to note that not all vulnerabilities are created equal, and a vulnerability discovered in voting equipment doesn't automatically equate to it being exploitable, especially at scale.

What are the security methods protecting voting equipment from any vulnerabilities being exploited?

Each of the participating manufacturers complies with federal testing and certification standards known as the Voluntary Voting System Guidelines (VVSG), which are approved by the U.S. Election Assistance Commission (EAC) in consultation with the National Institute of Standards and Technologies (NIST).

Under this robust testing program, voting systems must pass stringent testing by an independent, federally accredited Voting System Test Lab (VSTL) before any equipment can be fielded. Most states require compliance with these federal standards, and several states require rigorous additional state-level testing before approving systems for use.

Likewise, the participating manufacturers have all voluntarily subjected their voting systems to penetration testing conducted as part of CISA's Critical Infrastructure Testing Program.

Voting system manufacturers protect votes by deploying a multi-layered cybersecurity approach. For example:

- System hardening, role-based access, and multi-factor authentication are barriers against unauthorized access to election systems.
- Hardened and encrypted flash drives protect votes during transfer to election management systems and election authorities.
- Continuous cybersecurity training ensures manufacturers' personnel comply with the most effective cyber practices.

The physical security of voting systems is also a priority for election officials, using best practices such as:

- 24/7 video monitoring of equipment storage facilities.
- Secure containers that house the equipment during transport.
- Tamper-evident seals so that potential unauthorized access can be discovered.

What role does the government play in voting system testing and security?

Federal and state government authorities play a facilitating role in promoting security and overall confidence in elections by adopting and supporting sound principles of coordinated disclosure. Representatives of the U.S. Election Assistance Commission, National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and local officials with U.S. Homeland Security's Election Infrastructure Government Coordinating Council will take part in forum discussions.

EAC: The EAC Testing and Certification Program assists state and local election officials by providing voting machine testing and certification. This program is a requirement of the Help America Vote Act (HAVA) of 2002. The certification program independently verifies that voting systems comply with the functional capabilities, accessibility, and security requirements necessary to ensure the integrity and reliability of voting system operation, as established in the Voluntary Voting System Guidelines (VVSG).

NIST: The NIST Voting Program performs technical research to support the development of standards and guidelines for current and future voting systems. NIST major efforts are in the development of the Voluntary Voting Systems Guidelines (VVSG) through the Technical Guidelines Development Committee (TGDC) , which NIST chairs; accreditation of Voting Systems Test Labs (VSTL); research in accessibility and human factors, cybersecurity, and interoperability.

CISA: In January 2017, the Department of Homeland Security officially designated election infrastructure as critical infrastructure. CISA works collaboratively with public-private partners to manage risks to the nation's election infrastructure. The agency provides resources on election security for both the public and election officials at all levels to protect America's election infrastructure against threats.

Will there be another event of this kind?

This event culminates years of detailed planning by numerous entities, including manufacturers, third-party security advisors, election experts, and the IT-ISAC. The participants and the organizers will utilize the pilot event to help shape and guide any potential future events, which would occur after 2024.