IT ISAC

Elections Industry-Special Interest Group (EI-SIG)

Coordinated Vulnerability Disclosure Program White Paper

U.S. election systems manufacturers are cooperating and collaborating on timely initiatives to strengthen the security, reliability, and resilience of the nation's election infrastructure through the Information Technology-Information Sharing and Analysis Center (IT-ISAC) Elections Industry-Special Interest Group (EI-SIG). Protecting this critical infrastructure and its assets is a top priority for elections systems manufacturers, who support local, state, and federal elections nationwide.

This paper highlights the election systems manufacturer's voluntary efforts to establish an industry framework that identifies, assesses, and mitigates potential vulnerabilities in election systems. This joint industry initiative will serve as the evolutionary basis for a Coordinated Vulnerability Disclosure (CVD) program, assuming that its goals can be adapted and synchronized with state and federal testing and certification programs. This paper considers and explores:

- How a coordinated vulnerability disclosure program can help ensure the security of voting systems.
- How voting system testing and certification processes can support the voluntary adoption of CVD.
- Steps the industry will take to ensure the quality and effectiveness of the program.

COORDINATED VULNERABILITY DISCLOSURE

The U.S. Senate Intelligence Committee's July 2019 report urges the U.S. Department of Homeland Security (DHS) to "work with vendors of election equipment to educate them about the vulnerabilities in both the machines and the supply chains for the components of their machines."[1] This recommendation is notable because it recognizes that the industry is facing sophisticated, nation-state level threats. Given the nature of the threat, the industry is taking proactive measures to secure their systems. Even systems that are working perfectly well must be able to ward off more complex cyber threats. This is where coordinated vulnerability disclosure is useful.

In addition to enhancing voluntary information-sharing with DHS, the elections system manufacturer's initiative to establish a voluntary coordinated vulnerability disclosure program has several aims, including:

[1] U.S. Senate Intelligence Committee. (2019). "Russian Efforts Against Election Infrastructure." Retrieved from: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

- Provide trusted, repeatable processes to seek, identify, process, mitigate and disclose system vulnerabilities in a timely manner.[2]
- Expand upon existing federal and state processes for voting system certification, testing and reporting functions to strengthen product security and resilience.
- Educate key stakeholders – including government officials and the public – about how voting systems are designed, manufactured, tested and secured.

Elections system manufacturers share a common goal to develop a voluntary, industry-driven coordinated vulnerability disclosure program that applies the lessons from other industries to their unique market circumstances, which currently include a costly and time-consuming testing and certification process. This joint commitment to expanding and adapting product security practices by formally engaging with good faith researchers marks a significant turn in industry-wide thinking. Turning this support into formally coordinated vulnerability disclosure programs with corporate policies and procedures that will enable researchers to directly engage with impacted vendors to report, confirm, announce and fix vulnerabilities in coordinated fashion will require considerably more work ahead, including outreach to the researcher community, government regulators, and the public.

Fortunately, many resources and best practices already exist in other sectors of critical infrastructure to guide the industry in its work. In fact, Coordinated Vulnerability Disclosure is a common practice in many industries. Well designed and implemented coordinated vulnerability disclosure programs provide value for customers, vendors and researchers when everyone acts in good faith. If a vulnerability is announced before a fix is deployed and installed, the customer is at increased risk since attackers could try to exploit the publicly known, unpatched vulnerability. Vendors and customers benefit equally when a vulnerability can be fixed before it is exploited. Researchers also benefit when there is an easy, repeatable way for them to disclose a suspected vulnerability for an obvious reason--the less time they need to spend reporting vulnerabilities, the more time they can spend finding them. According to a survey by the Department of Commerce’s NTIA, 92% of researchers surveyed “generally engage in some form of coordinated vulnerability disclosure.”[3]

For these reasons, the elections systems manufacturers and its security partners at the IT-ISAC, have developed a Resource Guide to assist companies in building a corporate vulnerability disclosure plan and other next steps towards supporting CVD. Providing a resource guide will enable companies to more easily identify the practices and procedures that are most appropriate for their organization and maturity level as a Critical Infrastructure (CI) operator. The guide can be updated as more practices and policies are created.

[2] For purposes of EI-SIG discussions, and consistent with the Common Weakness Enumeration definition, a “vulnerability” is an occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness. See https://cwe.mitre.org/data/definitions/1000.html.

[3] Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group. Retrieved from: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

CROWD-SOURCED BUG BOUNTY PROGRAMS

In addition to establishing an industry-led Coordinated Vulnerability Disclosure Program, elections systems manufacturers of the EI-SIG are also looking into developing a crowdsource-style "Bug Bounty" program. The group is openly seeking ideas from experts and partners on how to effectively tailor and apply such a program for this unique industry. Consequently, building a process to adequately and appropriately vet researchers, and enacting effective policies to govern how the sector eventually provides these vetted researchers access to election systems is top of mind for the group.

For cybersecurity testing of network-connected systems such as voter registration (VR) systems, election night reporting (ENR) systems and electronic poll books, their online operating environment lends itself to so-called crowd-sourced "Bug Bounty" programs. Since researchers are often compensated based on the severity of the vulnerabilities they find, they have an incentive to identify and report more severe vulnerabilities and honor the confidentiality agreements that are part of the program. The fact that the researchers are vetted and bound to confidentiality agreements provides added assurances to companies that information will not be mis-used and discovered vulnerabilities will not be disclosed without authorization.

However, for voting systems (which are designed to be closed, isolated networks), applying crowd-sourced "Bug Bounty" testing is not as simple. Because it is not possible to upload a voting machine to a secure platform for researchers to investigate without creating new vulnerabilities and security issues, they do not easily lend themselves to crowd-sourced testing platforms.

To ensure that the best approach is adopted and in order to increase the security of election industry products, the elections manufacturers plan to seek comments and input from subject matter experts, key stakeholders and the public. The IT-ISAC EI-SIG is working on a draft Request For Information (RFI) to be released in the Fall of 2019.

SUPPORTING CVD ADOPTION FOR ELECTION INFRASTRUCTURE

While coordinated vulnerability disclosure is a well-established practice in other areas of critical infrastructure, the elections industry has some unique challenges that can only be overcome through collaboration across the Election Infrastructure Subsector (EIS). This is particularly true for voting systems manufacturers, who face a new layer of complexity in adopting CVD and will need to work with federal and state testing and certification authorities to avoid complicated, time-consuming and prohibitively expensive patching or updating scenarios.

As previously noted, essential software is not necessarily connected to the Internet in the elections space. Unlike most IT products, voting systems are designed to *not* connect to the Internet. This can make it very challenging to update or patch products as no "over the air" process exists. In many cases, an entire voting system may have to be retested or recertified in order to update or patch a single component, such as a workstation computer, router or server, to ensure that no unintended consequences or new vulnerabilities result from the upgrade. Under current federal requirements, a change to even one byte of the trusted software built in voting machines or back office computers requires re-testing. The entire process can take several weeks at best, and months to a year or more if problems are encountered.[4]

A related challenge is defining vulnerabilities and their severity. Given the relatively new critical infrastructure designation for elections, the community as a whole has not yet reached a common understanding as to what constitutes a system vulnerability or how to prioritize their impacts on the conduct of an election. For example, just because a vulnerability is identified in an off-line or disconnected voting machine, does not mean that vote tallies can be changed or manipulated. Often there are well established and proven compensation controls which effectively mitigate lower level vulnerabilities until a full update can be applied. In many cases, state election authorities would be crucial in determining upgrade pathways and timing. Considering the costs and timelines associated with deploying patches, the election community as a whole must consider ways to streamline the recertification process and reach consensus on how to determine and prioritize the severity of vulnerabilities.

Last, but certainly not least, establishing robust CVD practices for elections will require a great deal of stakeholder outreach and public education, so as not to impact confidence and trust in election outcomes. As noted, the existence of a voting system vulnerability does not mean that vote tallies can be changed or manipulated. However, that may be exactly how nefarious actors or even members of the public respond to such a revelation. Because so much of voting is personalized, politicized and more public than in other areas of technology, there are many concerns about how voting system vulnerabilities will impact the jurisdictions and voters who are impacted.

The election systems manufacturers are committed to building voluntary, industry-supported CVD programs that provide researchers and academics the opportunity to confidentially disclose vulnerabilities. However, this effort will only be successful if it is accompanied by changes that streamline and modernize the elections infrastructure. A CVD program is of limited value if the patches cannot be deployed in a timely and cost-effective manner. Specifically, the election systems manufacturers encourages:

- Federal and state election authorities with responsibility for testing and certification to develop a process for emergency incorporation of mitigations to critical vulnerabilities without negatively impacting system certification status.
- Incentives for industry to upgrade technology on a regular basis, and a standard “go/no-go” window around the conduct of live elections.

[4] There are three steps to the process - the first being Federal testing and certification, followed by state testing and approval, with the final step being coordination with the local end users to manually apply each update. As such, the elapsed time from when a fix is developed to the time the fix is approved, implemented and elections officials are trained on the updated machines could be a year or more.

- The crucial need for both certification programs and contractual parties to formulate and account for the lifecycle of an election system when considering upgrade pathways, maintenance options and vulnerability remediation.

ENSURING THE QUALITY OF CVD IN ELECTIONS

EI-SIG members have consulted with other industries to inform decision-making on CVD options for elections industry providers. In early 2019, the IT-ISAC hosted a day-long discussion between election companies and a variety of executives from other industries and ISACs**.** The goal was to learn how other industries have successfully partnered with the security research community in recent years to enhance the security of their products in today's global threat environment. A major point of emphasis was the value of working with ethical and properly-vetted security researchers to find a common mission.

More recently, EI-SIG company representatives met with leading crowd-sourced and vulnerability discovery service providers. The industry also engaged in discussions with leaders from federal and state government as part of a congressional roundtable. These discussions have been immensely valuable and have affirmed the industry's commitment to continuing its engagement with outside partners.

In addition to engagement through the EI-SIG, voting systems manufacturers take comprehensive measures to protect election systems. This includes the use of recognized security practices, as well as proprietary measures to secure their unique systems. Further, all elections systems undergo testing through state, local and federal election officials. For example, voting systems are tested and certified at the federal level by the U.S. Election Assistance Commission (EAC). The battery of tests which are conducted during the certification process provides useful information about the correct functioning of a voting system and its various components. Systems are then tested again at the state level, which can involve additional checks, such as penetration testing or red teaming the system. Some providers have taken the voluntary step of working with third-party security providers, academic institutions and federal government labs to test and study their systems and their vulnerabilities to malicious attacks.

CONCLUSION

Election system manufacturers have acknowledged the industry's role in responsibly ensuring that U.S. voting technology is secure and resilient in the face of dynamic, global threats. As part of this collective commitment, companies are building corporate CVD programs and are voluntarily engaging with relevant security partners. Companies are seeking input on crowd-sourced programs that could enable trusted, verified researchers to review voting systems and confidentially report suspected vulnerabilities, as well as red teaming scenarios that will meet voting system manufacturer needs for testing closed and non-networked, embedded systems.

Effectively implementing CVD programs throughout the elections' ecosystem can only be accomplished by working with federal and State Local Territorial and Tribal partners. There are a number of challenges that still need to be addressed before CVD programs can become as impactful as they need to be, including time-consuming and costly testing and certification processes, as well as voter and election official education to understand the benefits of CVD and what vulnerability remediation truly entails in this space. Elections systems manufacturers are committed to engaging with partners across the elections infrastructure to ensure the Elections Industry Subsector is are secure and resilient.

Coordinated Vulnerability Coordination Resource Guide

Working through the IT-ISAC EI-SIG, elections systems manufacturers have identified the below set of resources to assist members in voluntarily building out corporate vulnerability disclosure programs. The purpose of this Resource Guide is to identify industry accepted practices and procedures that companies can consult and reference as they build their coordinated vulnerability disclosure programs. The Resource Guide does not claim to be an all-inclusive set of practices and policies and elections systems manufacturers may, at their discretion, use guides or practices not identified in this Resource Guide. However, this Guide provides a common framework from which election systems manufacturers can build their coordinated vulnerability disclosure policies.

International Standards Organization: ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges.

- **International Standards Organization/IEC 29147-2018:** This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1].

- **International Standards Organization/IEC standard 30111:** This document gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

Forum of Incident Response and Security Teams (FIRST): FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

- **FIRST PSIRT Services Framework:** The Services Frameworks are high-level documents detailing possible services that computer incident response teams (CSIRTs) and product incident response teams (PSIRTs) may provide. They are developed by recognized experts from the FIRST community.

  FIRST also developed training content to assist companies in developing PSIRT Teams. Developed by FIRST's own PSIRT committee the materials are aimed at inhouse teams responsible for identifying and responding to product vulnerabilities. The purpose of the training is to demonstrate the differences and requirements management and stakeholders should be aware of to fully realize the potential of a PSIRT to their organization.

- **FIRST Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure:** This document differs from the ISO Vulnerability disclosure and handling standards (ISO/IEC 29147 and ISO/IEC 30111) in that the ISO standards provide basic guidance on the handling of potential vulnerabilities in products. This document is a collection of best current practices that consider more complex and typical real-life scenarios that extend past a single researcher notifying a single company about a discovered vulnerability.

CERT/CC: The CERT Guide to Coordinated Vulnerability Disclosure: This guide provides an introduction to the key concepts, principles, and roles necessary to establish a successful CVD process. It also provides insights into how CVD can go awry and how to respond when it does so.

Industry Consortium for Advancement of Security on the Internet (ICASI): The Industry Consortium for Advancement of Security on the Internet (ICASI) enhances the global security landscape by driving excellence and innovation in security response practices, and by enabling its members to proactively collaborate to analyze, mitigate, and resolve multi-stakeholder, global security challenges. The Unified Security Incident Response Plan (USIRP) is one of the primary means by which ICASI fulfills its mission of enhancing the global security landscape. The USIRP enables Security Incident Response Teams (SIRTs) from ICASI member companies to collaborate quickly and effectively to resolve complex, multi-stakeholder Internet security issues. The USIRP works by harmonizing ICASI member companies' internal security incident response procedures and personnel by providing a common, formal framework with which these organizations can: trigger a USIRP event, share critical information about it, and work together effectively on a coordinated response.

The Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct: The Committee on Professional Ethics (COPE) is responsible for promoting ethical conduct among computing professionals by publicizing the Code of Ethics and by offering interpretations of the Code, planning and reviewing activities to educate membership in ethical decision making on issues of professional conduct, and reviewing and recommending updates to the Code of Ethics and its guidelines.