

In September 2023, the IT-ISAC's Election Industry Special Interest Group (EI-SIG), with the guidance of an independent Advisory Board, facilitated the Election Security Research Forum (ESRF). Hosted at MITRE Corporation's National Election Security Lab, the ESRF was a pilot that provided the opportunity for qualified security researchers to engage with modern, pre-deployment voting technology provided by three voting technology providers who are members of the IT-ISAC Election Industry SIG—Election Systems & Software (ES&S), Hart InterCivic and Unisyn Voting Solutions. While no rewards or bounties to researchers were given as part of this event, funding for researcher travel was provided by the Center for Internet Security. Transparency in elections breeds trust — it is our hope that this event can serve as the starting point for more collaboration to come to safeguard our most valuable democratic processes.

As a condition of participation, all companies and researchers agreed to participate under the terms of Coordinated Vulnerability Disclosure (CVD). As is standard industry practice, these terms allow researchers to publicly disclose vulnerabilities after a set period of time has passed or the vulnerability has been fixed (see the "Coordinated Vulnerability Disclosure Process" section for more detail of the terms).

While coordinated vulnerability disclosure is a standard practice in most industries, the event organizers acknowledge the decades of contention between security researchers and voting technology providers. This will not change overnight. Nevertheless, this event served as the first time in which voting technology providers gave security researchers full access to modern voting equipment under the principles of coordinated vulnerability disclosure — meaning that researchers did not sign non-disclosure agreements (NDAs), are allowed to publicly disclose vulnerabilities in accordance with the vulnerability disclosure policies of the respective providers (see the appendices for copies of these policies), and received legal safe harbor in return for adhering to the vulnerability disclosure policies.



The ESRF represents five years of work by the IT-ISAC and its Election Industry SIG, which was formed in 2018. The SIG set the goal of building trusted engagement between industry and researchers based on the principles of coordinated vulnerability disclosure (CVD), allowing researchers to test modern election technology provided by SIG members at an in-person event.

The timeline that led to the ESRF pilot program is as follows:

- August 2018: The Elections Industry Special Interest Group is formed.
- October 2018: EI-SIG members agree that the group's primary goal is to develop an industry-specific coordinated vulnerability disclosure program.
- January 2019: EI-SIG has its first in-person meeting at BAE Systems in Tysons Corner to discuss coordinated vulnerability disclosure in various industries with guest speakers from the automotive, aviation, and medical industries.
- June 2019: EI-SIG met at BAE Systems in Annapolis Junction, MD and received presentations from a variety of companies, including Bugcrowd and HackerOne, about implementing CVD programs and engaging with researchers.
- August 2019: EI-SIG releases a white paper that covers how a CVD program can help ensure the security of voting systems, how voting system testing and certification processes can support the voluntary adoption of CVD, and steps the industry will take to ensure the quality and effectiveness of the program.
- **September 2019:** Following the white paper release, the EI-SIG publishes a Request for Information (RFI) to solicit feedback on how crowd-sourced CVD programs could be implemented in the elections industry.
- **December 2019:** EI-SIG reviews and discusses all RFI responses submitted to identify the best path forward. The SIG decides to form an Advisory Board comprised of leaders from the researcher and CVD communities.



- February 2020: The EI-SIG establishes an Advisory Board to help guide the industry's efforts. The Advisory Board provides subject matter expertise and guidance to the EI-SIG as the SIG develops policies, processes, and programs to enable and enhance coordinated vulnerability disclosure programs throughout industry.
- March 2020 April 2022: The COVID-19 pandemic and the 2020 elections provided some disruption in planning, but the SIG kept meeting virtually every other week.
- August 2020: IT-ISAC EI-SIG member companies release their first CVD Policies, which are published on the IT-ISAC website. This represented a large-scale shift towards advancing CVD in the elections industry.
- May 2022: The EI-SIG met in person at MITRE with members of the Advisory Board to implement a program plan for the SIG to host a pilot event with security researchers under the principles of CVD, with the goal of having the event in 2023.
- March 2023 September 2023: Participating companies, planners, and Advisory Board members met weekly to plan and implement the ESRF.
- September 18 20, 2023: The Election Security Research Forum pilot was held at MITRE Corporation.

## 

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. Bugcrowd and HackerOne, both leading bug bounty platforms who are members of the Advisory Board, identified researchers active on their platforms with hardware and software hacking skills for participation. Several researchers have previous experience researching election technology, including at the DEF CON Voting Village. Researchers who have been involved in litigation related to election technology companies were not invited to participate due to potential conflicts their participation would create.



With three diverse companies participating in the event, researchers received access to a variety of election technology. Each company determined what hardware they made available for the event. The robust offering of equipment provided collectively included digital ballot 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 software and hardware tested at the pilot forum had yet to be deployed in a live election — offering a crucial opportunity to proactively identify potential security weaknesses prior to deployment. Some hardware presented at the forum may already be in use, while other hardware has yet to be introduced into the market.



### THE ADVISORY BOARD

The IT-ISAC organized an independent Advisory Board to help guide the development and implementation of the ESRF. The role of the Advisory Board was to serve as a bridge between the security community and the election technology providers, including identifying qualified security researchers and helping ensure the ESRF was structured and developed in a way that would add value to the security researchers and the participating companies.

The Advisory Board members for the 2023 event were:

- · Jared Dearing, Center for Internet Security
- Casey John Ellis, Co-Founder and CTO, Bug Crowd
- Matthew Masterson, Microsoft
- · Chloé Messdaghi, Head of Threat Intelligence, HiddenLayer
- 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



The event was structured to allow researchers to freely tinker with the election technology. The event began with an "Elections 101" presentation by The Elections Group, which gave researchers an overview of electoral processes, threat models, and the role of various election technologies. This was followed by a discussion by each vendor about the equipment that they brought. Following that, researchers had a day and a half with access to the machines.

During the testing periods, each provider had their own room for their equipment, and researchers were able to move between rooms as they preferred. Some providers designated certain devices for destructive testing, to which researchers could act as they pleased, with other devices serving as models for how they should function in a normal election. Initially, researchers were given no additional access (e.g. credentials) to the machines, while over time, some providers gave researchers elevated access to simulate threat scenarios such as insider compromise.

# COORDINATED VULNERABILITY

One of the underlying principles of this event was that security researchers who volunteered their time for the event should be able to do so without fear of legal action and publicly disclose their findings. Building on prior work on vulnerability disclosure in election systems, the election technology providers developed vulnerability disclosure policies. These policies provide legal safe harbor to researchers in exchange for adhering to the policies, and do not place arbitrary restrictions on the disclosure of vulnerabilities. Rather, the policies allow for researchers to publicly disclose vulnerabilities after either a set timeframe has passed, and/or the vulnerability has been fixed.

Note: Some of the providers' policies do differ from standard coordinated vulnerability disclosure practices in that they may ask researchers to not disclose vulnerabilities even after 120 days if the vulnerability has yet to be patched. This is due, in part, to unique state and federal certification requirements in elections, which may delay patches from being made available and fielded. The intent of CVD is dually to build trust through transparency and prevent harm to end-users. As such, the language is not meant to impede disclosure, but rather to establish open lines of communication and set clear expectations as patches are developed and fielded. This remains an open area for further discussion and we welcome input on how to best balance this.



As noted, the goal the IT-ISAC Election Industry SIG set initially was to build a trusted framework in which security researchers and election technology providers can engage under the principles of Coordinated Vulnerability Disclosure. In this regard, the event was unquestionably a success and laid the foundation for future collaboration.

This event sought to demonstrate that collaboration between security researchers and election technology providers is not only possible, but beneficial towards securing our electoral processes. It is imperative to build security and resilience into these systems, implement mitigations, and manage risk while working collaboratively. The goal of the event was not to prove the absence of vulnerabilities, nor to systematically identify all vulnerabilities in the election systems. Events such as this are trying to identify vulnerabilities so that they can be addressed.

Researchers reported their findings to the participating companies after the event. The participating companies and security researchers continue to collaborate to confirm and address what was reported. Participating companies have released their findings from the event and can be found below.

- <u>Election Systems & Software (ES&S)</u>
- Hart InterCivic
- <u>Unisyn Voting Solutions</u>

It is our hope that this is seen as a positive step towards normalizing the process of CVD in elections — not some proof that vulnerabilities were exploited or that elections are not secure. Indeed, the voting equipment used in this pilot was equipment that is not yet certified and has not been fielded. These systems have not been used in any election.

In reality, every critical infrastructure domain faces risk and has vulnerabilities. Our banking systems, technology providers, and other critical infrastructure all have vulnerabilities. This is not reason to distrust these systems.

The event demonstrated the value of collaboration. Prior to the event, the voting technology providers were understandably nervous about opening up their systems and were unsure how to provide the right levels of openness and collaboration. In the short time span of the event, the voting technology providers and their operational and technical staff became much more open to collaboration between researchers and began offering more aid (such as helping understand their systems or providing administrative credentials). Researchers appreciated the collaborative spirit (with some noting that this was the most collaborative live hacking event they had participated in).



Amidst heightened distrust in elections, it is even more important to normalize the process of CVD, building positive working relationships between researchers and election technology providers, and demonstrating this collaboration to the public.

Over the course of the three-day event, it was clear that there was significant trust built between the participating researchers and the voting technology providers. Transparency in elections breeds trust — it is our hope that this event can serve as the starting point for more collaboration to come to safeguard our most valuable democratic processes.

The organizers recognize that a day and a half of testing is not equivalent to an adversary with unlimited resources. Giving researchers elevated access, as did several of the participating companies, is one way to close the gap between the limited time the researchers had and the capabilities of a well-resourced adversary. We hope to build on this work with future events to further help protect these voting systems.

The ESRF also identified several policy issues that need to be addressed by the larger election security community and policymakers. For instance, we recognized the need to update and modernize the process of testing and certifying election technology for use in the field so that any vulnerabilities or security issues identified on deployed election technology can be resolved and deployed to fielded systems quickly. Until this happens, it may continue to be the case that certification delays the patching of election technology.



Following the success of this event, the Advisory Board and IT-ISAC Election Industry SIG members are actively working with the larger election community on the appropriate next steps. In 2024, the group will focus on identifying ways to update and modernizing the certification process to account for CVD programs within the industry and developing a framework for future iterations of this event.

The organizers believe the ESRF was successful and are hopeful that an expanded event could occur in 2025. This follow-up event will likely include participation from a broader set of researchers and participation from additional companies and other elements of the larger election ecosystem, including state and local election officials. If you are a researcher, election technology provider, or election official interested in participating, please email the IT-ISAC at CVD@IT-ISAC.ORG. Our goal is to normalize the process of CVD in elections, achieving a future state in which independent good-faith security research on voting technology is commonplace, and everyone can benefit from the greater security and trust that is fostered.



The following CVD policies were in place for the 2023 ESRF event and provided to all researchers.

#### A: Election Systems & Software (ES&S)

ES&S Vulnerability Disclosure Policy

#### **B: Hart InterCivic**

Hart InterCivic Vulnerability Disclosure Policy

#### **C: Unisyn Voting Solutions**

<u>Unisyn Vulnerability Disclosure Policy</u>

#### **D: Researcher Participation Form**

As part of the event, researchers signed a participation form, modeled after participation forms from other events. This form is not an NDA, but rather laid out the values of the event, including CVD, and event ground rules, including physical safety, CVD, and external communications. Form here.

The Elections Industry - Special Interest Group (EI-SIG) is part of the Information Technology - Information Sharing and Analysis Center (IT-ISAC). The EI-SIG is compromised of election of voting technology providers and and gives them an industry-only forum to share information about threats to their enterprises and systems and collaborate on election security challenges.

#### IT-ISAC.ORG/EI-SIG CVD@IT-ISAC.ORG

