U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Dear EAC Awards Committee Members:

Thank you for the opportunity to submit the Iowa Bug Bounty program for the 2022 Clearinghouse Award in the category of Outstanding Innovation in Election Cybersecurity and Technology. For the last several years, my office has made a concerted effort to continually bolster our election cybersecurity. Our Vulnerability Disclosure Program and Bug Bounty program are the latest initiatives in this ongoing effort to ensure our elections infrastructure is secure at every level.

Iowa is at the forefront of state election offices utilizing bug bounties to protect elections. We collaborated with Bugcrowd, a national leader in crowdsourced cybersecurity, to identify ethical security hackers that can responsibly look for vulnerabilities in our systems and report them to us. Similar programs are utilized within the federal government and several fortune 500 companies.

This effort is a crucial step in our ongoing efforts to enhance election cybersecurity and I believe every election office in the country should consider a similar initiative.

Thank you very much for your time and consideration.

Sincerely,

Paul D. Pate

Paul D. Pate, CERA
Iowa Secretary of State

U.S. Election Assistance Commission Award Application 2022

Iowa Secretary of State's Office

Outstanding Innovation in Election Cybersecurity and Technology

State Office: Iowa Secretary of State Paul D. Pate

Contact: Michael Ross, Deputy Chief of Staff; (515) 725-2874, Michael.Ross@sos.iowa.gov

Title of Program: *Vulnerability Disclosure and Bug Bounty program*

Project lead: Kyle Phillips, Chief Information Officer; Michael Ross, Deputy Secretary of State

Subject area of nomination: Outstanding Innovation in Election Cybersecurity and Technology

EXECUTIVE SUMMARY

Election cybersecurity remains a race without a finish line. To that end, there is growing momentum in election offices around the country to institute Vulnerability Disclosure Programs and Bug Bounty programs to help election officials bolster their cyber maturity. The Iowa Secretary of State's Office became the first election office in the nation to launch a Bug Bounty program. We offer monetary rewards to security researchers who find vulnerabilities in websites maintained by the Secretary of State's office.

Our Bug Bounty program launched in 2022, ahead of the November general election. It was a valuable addition to Iowa's Vulnerability Disclosure Program (VDP) which launched in 2020. We were the second state election office in the country to launch a VDP.

The Iowa Secretary of State collaborated with Bugcrowd, a national leader in crowdsourced cybersecurity, for this initiative. Iowa operates its Vulnerability Disclosure Program (VDP) as part of the core cybersecurity framework recommended by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Adding a Bug Bounty program enhances our protections.

A Bug Bounty program entails offering ethical security hackers recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse and data breaches.

The value of a Bug Bounty program is a proactive approach to securing websites and applications. Without a Bug Bounty program, organizations are left to find vulnerabilities through their own scanning and penetration testing efforts, or by being breached. Having a Bug Bounty program is akin to having a penetration test 24 hours a day, seven days a week, 365 days a year. A typical pen test is one or two weeks out of the year. The Bug Bounty program allows for a wide range of talent and approaches to finding vulnerabilities, versus one or two pen testers.

Bug Bounty programs and Vulnerability Disclosure Programs are regarded as additional countermeasures to thwart threat actors. Cybersecurity is most effective when done in layers. Firewalls, intrusion detection, and anti-virus measures are examples of some of these layers. The Bug Bounty program is an important additional layer.

Protecting elections with proven cybersecurity controls is a top priority for the Iowa Secretary of State's Office. Forging and building upon critical partnerships with federal, state, and local authorities as well as private sector industry leaders allows for continuous improvements to Iowa's election infrastructure.

EI-ISAC is piloting a VDP program to offer to election offices at no charge because they recognize the significance of this security control. More and more election offices (and entire state governments) are taking on VDP and Bug Bounty programs and Iowa is on the leading edge of this movement.

Similar programs are utilized within the federal government and several fortune 500 companies. This includes Facebook, AT & T, Apple, Google, Microsoft, and federal government agencies like the U.S. Department of Homeland Security, the U.S. State Department, and the U.S. Department of Defense.

Dozens of researchers have partnered with the Iowa Secretary of State's Office on this venture. The benefits of a Bug Bounty program to an election office are numerous. It protects publicly available election and voter registration applications, and websites. A successful website or application breach could allow threat actors direct access to Iowa's election and voter registration infrastructure. Any breach would be a serious threat to the reputation and trust of the Secretary of State's office and could cause catastrophic damage to voter confidence in Iowa's election systems.

BACKGROUND

The Bug Bounty program is an extension of Iowa's VDP, which launched in 2020. Iowa was the second state in the nation to create a VDP, inviting private sector security researchers to test Iowa's system. We are the first to institute a Bug Bounty program to provide recognition and monetary compensation to researchers who discover and report vulnerabilities to us.

A Vulnerability Disclosure Program is a structured framework for security researchers to document and submit security vulnerabilities to organizations. Vulnerability Disclosure Programs help organizations mitigate risk by supporting and enabling the disclosure and remediation of vulnerabilities before hackers exploit them.

Vulnerability Disclosure Programs enable users to perform technical vulnerability management and help users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. For elections, this is crucial.

Iowa's Bug Bounty program launched ahead of the 2022 general election. It was yet another proactive measure to ensure our elections are cyber secure. We are actively engaging the private security researcher community so we can strengthen our systems and ensure Iowa continues to be a leader in elections and cybersecurity.

ACTION STEPS

Finding new and innovative ways to protect elections is a top priority for election officials across the country. A VDP and Bug Bounty program are the latest steps in this effort. We contracted with Bugcrowd, a national leader in crowdsourced cybersecurity, to assist with finding ethical security hackers to look for potential vulnerabilities and report them to us.

"We are excited to partner with the State of Iowa to proactively counter cyber threats with the help of a crowd of researchers that specialize in election security, ensuring a strong and resilient cybersecurity posture and force multiplier to safeguard elections," said Bugcrowd CEO Ashish Gupta.

For a VDP to be successful, it generally requires the engagement and interest of ethical hackers. Ethical hackers "hack" into a computer network to test and evaluate security but do so without any malicious or criminal intent and generally have the cooperation of the targeted organization.

Ethical hackers must take the perspective of malicious threat actors. They step into the shoes of threat actors and view an organization's defenses from the perspective and mindset of a potential attacker. Ethical hackers must take active measures to probe cyberdefenses for vulnerabilities that would allow them to position a successful cyberattack. The success of ethical hackers in identifying vulnerabilities reduces or eliminates the potential opportunity for the next real malicious threat actor.

Interaction with ethical hackers must be subject to essential ground rules agreed upon between the ethical hacker and the organization. Vulnerability disclosure policies document the most critical engagement ground rules, including safe harbor sections declaring an organization's commitment not to take legal action for security research activities that follow a good faith effort to follow the policy.

The language recommended by CISA for a government agency's vulnerability disclosure policy authorization and safe harbor is:

"If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and AGENCY NAME will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known."

Other guidelines further set the boundaries of the rules of engagement for ethical hackers. Guidelines may include an explicit request to provide notification as soon as possible after discovering a potential security vulnerability. Exploits should only be used to confirm a vulnerability. Many vulnerability disclosure policies request that discovered exploits not be used to compromise data further, establish persistence in other areas, or move to other systems.

A best practice is to allow ethical hackers the option of submitting vulnerability reports anonymously. In this case, the vulnerability disclosure policy would not require the submission of identifying information.

The Iowa Secretary of State chose a coordinated disclosure program, which signals a willingness to consider public disclosure of remediated vulnerabilities. This disclosure may be in whole or redacted form and may be determined on a case-by-case basis.

VDPs reduce risk by enabling you to accept, triage securely, and rapidly remediate valid vulnerabilities submitted from the security community. Statistics have shown that 87% of organizations have received a critical or high-priority vulnerability through a VDP.

Bug Crowd has an existing network of more than 100,000 security researchers. They also provide the platform for reporting and tracking submissions. Bugcrowd also triages submissions to filter out ones that are duplicates, not reproducible, and out of scope of the project. They also set the severity levels of the submissions-low, medium, high, and critical.

Bugcrowd does the heavy lifting in managing the Vulnerability Disclosure Program and Bug Bounty program for us.

RESULTS

Since deploying Iowa's Vulnerability Disclosure Program in 2020, we've had 46 vulnerabilities reported to us. More recently, after the launch of the Bug Bounty program, a cybersecurity researcher discovered a vulnerability in a vendor's system who maintains election websites for several Iowa counties. Had this vulnerability been discovered by a malicious actor, the consequences could have been disastrous for Iowa's elections. Thanks to this discovery from an ethical hacker, it was quickly reported and fixed.

We also have also had submissions for multiple election-related websites operated by our office, including our one-stop shop for election-related information, VoterReady.Iowa.gov. Those reports have improved the security of those sites.

Our initial Bug Bounty program includes a full ransom of $25,000. To date, we have paid out almost $9,000 to ethical hackers who have reported vulnerabilities to us. After two and half years of working with Bugcrowd, our cost to them has been approximately $170,000. Although that sum might seem like a lot at first glance, this is a fantastic return on investment.

A malicious actor hacking into one of the websites could have caused significant damage to voter confidence that could not be quantified in monetary value. Additionally, ransomware bounties have cost government entities millions of dollars in recent years. Having an ethical hacker find the vulnerability and giving them a monetary reward is much more cost effective and cybersecure.

Following the success of our Bug Bounty program, the Iowa Secretary of State is launching a separate, but related Bug Bounty program with county I.T. directors to ensure every county in Iowa has top notch cybersecurity and our elections are protected on every level.