Vulnerability disclosure policy

The Office of Iowa Secretary of State takes the security of our systems seriously. We value the security research community and believe by working together we can help ensure the security and privacy of our users, our systems, and our data.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered, as set out in this policy, so that we can fix them and keep the public's information safe.

This policy describes the systems and types of research are covered under this policy, how to report vulnerabilities to us, what we ask of researchers, and what researchers can expect from us.

Guidelines

We require that you:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data during security testing;
- Only test to the extent necessary to confirm a vulnerability in systems identified within the scope section below. Do not compromise or exfiltrate data, establish command line access and/or persistence, or "pivot" to other systems. Once you've established that a vulnerability exists, or encounter any of the sensitive data outlined below, you must stop your test and notify us immediately;
- Use the identified communication channels to report vulnerability information to us; and,
- Keep confidential any information about discovered vulnerabilities for at least 90 calendar days after you have notified the Office of Iowa Secretary of State. For details, please review Coordinated Disclosure below.

Scope

This policy applies to the following systems:

- sos.iowa.gov
- filings.sos.iowa.gov (which is synonymous with filing.sos.iowa.gov, filings.iowa.gov, filing.iowa.gov
- safeathome.iowa.gov
- api.sos.iowa.gov

Any services not expressly listed above, including any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy. If you aren't sure whether a website, system, or endpoint is in scope or not, contact us at support@bugcrowd.com before starting your research.

The following test types are not allowed:

- Denial of service (DoS or DDoS) tests.
- Physical testing (e.g. office access, open doors, tailgating).
- Social engineering (e.g. phishing, vishing).
- Defacement

Testing considered out of scope:

- We ask that testers avoid intentionally or potentially disruptive test types, including but not limited to DNS spoofing or DNS tunneling.
- Functionality bugs, clickjacking, email spoofing, etc. are considered out of scope. Our intent is to work with researchers to identify software and system vulnerabilities, not to identify low impact issues. Testers may report such issues, but they may not be handled as an issue subject to this vulnerability disclosure process.

Sensitive Information

If you encounter any of the below on our systems while testing within the scope of this policy, stop your test and notify us immediately:

- Personally identifiable information (social security numbers, driver's license numbers, full date of birth)
- Financial information (e.g., credit card or bank account numbers)
- Sensitive voter registration information, and other information in Iowa Code chapter 715C: https://www.legis.iowa.gov/docs/code/715c.pdf.

Authorization

When conducting vulnerability research according to the Guidelines and Scope of this policy, we consider this research to be:

- Authorized in accordance with the Computer Fraud and Abuse Act (CFAA) (and/or similar state laws), and we will not initiate or support legal action against you for accidental, good faith violations of this policy;

- Exempt from the Digital Millennium Copyright Act (DMCA), and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in any software Terms & Conditions that would interfere with conducting security research, and we waive those restrictions on a limited basis for work done under this policy; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faithYou are expected, as always, to comply with all applicable laws.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please contact us through one of the channels in the "Reporting a vulnerability" section before going any further.

Reporting a vulnerability

We accept and discuss vulnerability reports through the web reporting form at the bottom of this page. Reports may be submitted anonymously[1]. Note: We do not support PGP-encrypted emails. For particularly sensitive information, submit through our TLS-encrypted web form.

Reports should include:

- Description of the location and potential impact of the vulnerability.
- A detailed description of the steps required to reproduce the vulnerability. Proof of concept (POC) scripts, screenshots, and screen captures are all helpful. Please use extreme care to properly label and protect any exploit code.
- Any technical information and related materials we would need to reproduce the issue.

Vulnerabilities in Office of the Iowa Secretary of State systems may be relevant to other state and local governments who use similar technology. We may share your vulnerability reports with U.S. federal, state, and local government agencies and the information sharing organizations that work closely with them. This sharing may include the U.S. Department of Homeland Security, the Cybersecurity & Infrastructure Security Agency (CISA), the Multi-State Information Sharing & Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), and the Office of the Iowa Chief Information Security Officer as well as any affected vendors or open source projects.

Acknowledgement of Reports

[1] If you wish to remain anonymous you may use a pseudonym and contact CDOS with a "throw-away" email account.

Bugcrowd will take action on your submittal within 3 business days of receiving it. We will work with them and you to validate the issue, understand the security impact of the finding and provide periodic updates where relevant.

When a vulnerability has been resolved, we will notify you. We will offer you the opportunity to test and verify that the remediation has been successful. The “Coordinated Disclosure” section below specifies our commitment to publishing vulnerabilities after reporting. We are not offering financial compensation or “bug bounties” as part of our program.

Coordinated Disclosure

Office of the Iowa Secretary of State is committed to resolving vulnerabilities in 90 days or less and may disclose the details of those vulnerabilities when they have been resolved. We believe that public disclosure of vulnerabilities is an essential part of the vulnerability disclosure process, and that one of the best ways to make software better is to enable everyone to learn from each other's mistakes.

At the same time, we believe that disclosure in absence of a readily available remediation tends to increase risk rather than reduce it, and so we ask that you refrain from sharing your report with others during the 90-day window while we work to resolve issues. If you believe there are others that should be informed of your report before it has been resolved, please let us know.

We may want to coordinate an advisory with you to be published simultaneously with the resolution, but you may self-disclose if you prefer. As a state office, communications with us are subject to Iowa’s open records law (Iowa Code ch. 22). Please inform us in the submission that you would like to remain confidential. If we believe it is lawful or there is an applicable exemption from the open records law, we will protect your information to the fullest extent possible. However, we cannot guarantee full confidentiality. In some cases, we may also have some sensitive information that should be redacted, and so please check with us before self-disclosing.

We support coordinated disclosure that advances the security of our systems. We will publicly acknowledge your research and disclosure if you wish.

Report a Vulnerability

https://sos.iowa.gov/vulnerabilitydisclosureprogram.html