Policy Number: 51.822
Effective Date: 03/12/2021

Vulnerability Disclosure Policy

Introduction

The U. S. AbilityOne Commission is committed to ensuring the security of the organization assets by protecting their information from disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered "as set out in this policy" so we can fix them and keep our public users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

Authorization

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 AbilityOne 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. However, nothing in this authorization includes any right to compensation to researchers reporting vulnerabilities to us or for any indemnification against any third parties. Furthermore, this authorization does not create any obligation on our part to compensate you for reporting any security vulnerabilities to us.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations (exposing data), degradation of user experience, disruption to production systems, and destruction or manipulation of data.

- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems.

- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly Technically validated submissions will be responded to within 3 business days. Valid vulnerabilities will be resolved by the resolution timeline:

Critical	For Internet-accessible IP addresses: within 15 calendar days of initial detection.
High	Within 30 calendar days of initial detection
Moderate/Medium	Within 90 days of initial detection
Low	No specific deadline unless defined by the Commission CIO

- Do not intentionally compromise the privacy or safety of U.S. AbilityOne Commission personnel (e.g., civilian employees or contractors), or any third parties.

- Do not intentionally compromise the intellectual property or other commercial or financial interests of any AbilityOne personnel or entities, or any third parties.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**, including the Vulnerabilities Equities Process (VEP) or other similar process.

Scope

This policy applies to the following systems and services:

- *.abilityone.gov

- *.oig.abilityone.gov

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-federal systems from our business partners fall outside of this policy's scope. You should report any

vulnerabilities related to those entities directly to the company according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact CyberSupport@Abilityone.gov before starting your research or at the security contact for the system's domain name listed in the .gov WHOIS.

Though we develop and maintain other internet-accessible systems or services, we ask that *active research and testing* only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Test Methods

Typical Vulnerabilities Accepted:

- OWASP Top 10 vulnerability categories
- Other vulnerabilities with demonstrated impact

The following test types are not authorized:

- Network denial of service (DoS or DDoS) tests
- Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing
- Social engineering or phishing of customers or employees
- Theoretical vulnerabilities
- Informational disclosure of non-sensitive data
- Low impact session management issues
- Self XSS (user defined payload)

Reporting a vulnerability

We accept vulnerability reports at CyberSupport@AbilityOne.gov and reports may be submitted anonymously.

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all

users of a product or service and not solely U. S. AbilityOne Commission, we may share your report with the Cybersecurity and Law Enforcement Agencies, where it will be handled under their *coordinated vulnerability disclosure process*. We will not share your name or contact information without express permission.

By emailing your report, you are indicating that you have read, understand, and agree to the guidelines described in this policy for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to U.S AbilityOne Commission information systems, and consent to having the contents of the communication and follow-up communications stored on a U.S. Government information system. By submitting a report of vulnerabilities, you also affirmatively waive any claims to compensation.

We do not support PGP-encrypted emails at this time. For particularly sensitive information, please contact us at 703-603-2100.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Adhere to all legal terms and conditions outlined
- https://www.abilityone.gov/laws,_regulations_and_policy /vulnerability-disclosure-policy.html
- Describe the vulnerability, where it was discovered, and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Do not engage in disruptive testing like denial of service or any action that could impact the confidentiality, integrity or availability of information and systems.
- Do not engage in social engineering or phishing of customers or employees.
- Do not request compensation for time and materials or vulnerabilities discovered.
- Be in English, if possible.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- If you share contact information, we will acknowledge receipt of your report within 3 business days.

- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.

- We will maintain an open dialogue to discuss issues you discover.

- We want researchers to be recognized publicly for their contributions, if that is the researcher's desire. We will seek to allow researchers to be publicly recognized whenever possible. However, public disclosure of vulnerabilities will only be authorized at the express written consent of U.S. AbilityOne Commission.

- Information submitted to U.S. AbilityOne Commission under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks or applications, or the applications of our vendors.

- We will neither compensate nor indemnify any researcher for any research or discovery of any vulnerabilities.

Questions

Questions regarding this policy may be sent to CyberSupport@AbilityOne.gov and we also invite you to contact us with suggestions for improving this policy.

U.S. ABILITYONE COMMISSION

Vulnerability Disclosure Policy

Document change history

Version	Date	Reviewed By	Description
0.1 Initial	03/11/21	R. Newman	First draft to align with directive.
0.2	2021	Ed Yang	Reviewed draft policy

APPROVED: _____**Date:** March 23, 2021

E. Ballard

Executive Director