

USAID Vulnerability Disclosure Policy

Introduction

The U.S. Agency for International Development (USAID) is committed to safeguarding our systems and sensitive information from unauthorized 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.

It describes **what systems and types of security 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 encourage security researchers to contact us to report potential vulnerabilities identified in USAID systems. For reports submitted in compliance with this policy, USAID will acknowledge receipt within 5 business days; endeavor to timely validate submissions; implement corrective actions, if appropriate; and inform researchers of the disposition of reported vulnerabilities.

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 and will work with you to understand and resolve the issue quickly, and USAID 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.

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. This includes but is not limited to the discovery of a vulnerability and / or the exposure of nonpublic data.
- Purge any stored USAID nonpublic data upon reporting a vulnerability.
- Do not delete, alter, share, retain, or destroy USAID data, or render USAID data inaccessible, and do not disclose any personally identifiable information encountered to a third party.
- Make every effort to avoid privacy violations, 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 persistent command line access, or use the exploit to pivot to other systems.
- Do not introduce malicious software.
- Disclose vulnerability information as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly (as set forth below).
- Do not submit a high volume of low-quality reports.
- Once you've established that a vulnerability exists or encounter any sensitive/nonpublic 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.

Test Methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing
- Testing any system other than the systems set forth in the 'Scope' section below

Scope

This policy applies to the following systems and services:

- feedthefuture.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 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 any). If you aren't sure whether a system is in scope or not, contact us at VDP@usaid.gov before starting your research.

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.

Reporting a Vulnerability

We accept vulnerability reports via electronic mail at VDP@usaid.gov. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 5 business days.

Researchers may submit reports anonymously or provide contact information and any preferred methods or times of day to communicate, as they see fit. We may contact researchers to clarify reported vulnerability information or other technical interchange.

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 USAID, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their [coordinated vulnerability disclosure process](#), as well as any affected vendors. We will not share your name or contact information without express permission.

By submitting a report to USAID, researchers warrant that the report and any attachments do not violate the intellectual property rights of any third party, and the submitter grants USAID a non-exclusive, royalty-free, world-wide, perpetual license to use, reproduce, create derivative works, and publish the report and any attachments.

What we would like to see from you

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

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- A description of any tools needed to identify or exploit the vulnerability.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful). It is helpful to give attachments illustrative names. We request that any scripts or exploit code be embedded into non-executable file types. We can process all common file types, and also file archives including zip, 7zip, and gzip.
- 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.

- Within 5 business days, we will acknowledge that your report has been received.

- 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.

Disclosure

USAID is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily-available corrective action likely increases versus decreases risk. Accordingly, please refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, please coordinate in advance with us.

Questions

Questions regarding this policy may be sent to VDP@usaid.gov. USAID encourages security researchers to contact us for clarification on any element of this policy. Please contact us prior to conducting research if you are unsure if a specific test method is inconsistent with or unaddressed by this policy. We also invite security researchers to contact us with suggestions for improving this policy.

Document change history

Version	Date	Description
1.0	February 22, 2021	First issuance