USAID Vulnerability Disclosure Policy

Overview

The U.S. Agency for International Development (USAID) is committed to safeguarding our systems and sensitive information from unauthorized disclosure. This Vulnerability Disclosure Policy (VDP) is intended to provide security researchers clear guidelines for conducting vulnerability discovery activities and to explain the process for submitting discovered vulnerabilities to USAID. Vulnerability identification and remediation is critical to enhancing USAID cyber resilience and managing the risks associated with a global digital technology footprint. A strong partnership with the broader security researcher community can enable USAID to take immediate corrective action on potentially critical threat vectors.

We encourage security researchers to read the entire policy prior to submitting a vulnerability disclosure report to ensure report submissions are compliant with this policy and contact the USAID VDP Team, vdp@usaid.gov, to report potential vulnerabilities identified in USAID internet-accessible systems. The policy describes **what systems are in scope, what types of security research** are covered under this policy, **how to send USAID** vulnerability reports, and **how long** USAID asks security researchers to wait before publicly disclosing vulnerabilities. For reports submitted in compliance with this policy, USAID will: acknowledge receipt within five (5) business days; endeavor to timely validate submissions; implement corrective actions, if appropriate; and inform researchers of the disposition of reported vulnerabilities.

Authorization

If a good faith effort is made 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, USAID will make this authorization known.

This policy does not grant authorization, permission, or otherwise allow expressed or implied access to USAID information systems to any individual, group of individuals, consortium, partnership, or any other business or legal entity. You must otherwise comply with all applicable Federal, State, and local laws in connection with your security research activities. You may not engage in any security research or vulnerability disclosure activity that is inconsistent with terms and conditions of this policy or the law. However, if any security research activities conducted

are inconsistent with the terms and conditions of this policy or the law, you will no longer be considered a “security researcher” and may be subject to criminal penalties and civil liability.

Scope

This policy currently applies to the following systems and services:

- childreninadversity.gov and uat.childreninadversity.gov
- *.dfafacts.gov
- feedthefuture.gov
- foreignassistance.gov
- monitor.net.co
- neglecteddiseases.gov and uat.neglecteddiseases.gov
- pmi.gov and uat.pmi.gov
- portal.azure.com
- prosperafrica.gov
- *.usaid.gov, and the following hostnames:
    - 2012-2017.usaid.gov
    - 2017-2020.usaid.gov
    - aamptest.usaid.gov
    - aaplan.usaid.gov
    - abacus.usaid.gov
    - aidscape.usaid.gov
    - blog.usaid.gov
    - claimsweb.usaid.gov
    - data.usaid.gov
    - dec.usaid.gov
    - dis.usaid.gov
    - disdev.usaid.gov
    - disreporting.usaid.gov
    - eads.usaid.gov
    - ecd.usaid.gov
    - explorer.usaid.gov
    - foiarequest.usaid.gov
    - ghsurveys.usaid.gov/cms
    - gh-usersguide.usaid.gov
    - gismigration.usaid.gov
    - idea.usaid.gov
    - mrr.usaid.gov
    - ngoportal.usaid.gov/NGO
    - oig.usaid.gov
    - otiaccess.usaid.gov

    - otianywhere.usaid.gov
    - otidatabase.usaid.gov
    - otipakdb.usaid.gov
    - otistaff.usaid.gov
    - otitomas.usaid.gov
    - pdf.usaid.gov
    - peter-manager.usaid.gov/
    - peter-responder.usaid.gov
    - programnet.usaid.gov
    - programnetuat.usaid.gov
    - results.usaid.gov
    - sbmart.usaid.gov
    - share.usaid.gov
    - stories.usaid.gov
    - tableau.usaid.gov
    - tcb.usaid.gov
    - teams.usaid.gov
    - uatweb.usaid.gov
    - usaidinfo.usaid.gov
    - utrams.usaid.gov
    - webta.usaid.gov
    - www-origin.usaid.gov
    - Any other subdomain of usaid.gov and all customer applications, not currently listed, are excluded from this policy
- workwithusaid.org

Any system or service not explicitly 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 are not sure whether a system is in scope or not, contact the USAID VDP team, vdp@usaid.gov, **before** starting your research.

Though USAID develops and maintains other internet-accessible systems and 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 USAID (vdp@usaid.gov) first. We will increase the scope of this policy over time.

Guidelines

Under this policy, "research" activities include:

- Testing, through remote means, to detect a vulnerability or identify an indicator related to a vulnerability.
- Sharing information with or receiving information from USAID about a vulnerability or an indicator related to a vulnerability.
- Notifying USAID as soon as possible after discovery of 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.
- Purging any stored USAID nonpublic data upon reporting a vulnerability.
- Disclosing vulnerability information as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below.
- Providing USAID us a reasonable amount of time to resolve the issue before you disclose it publicly (as set forth below).
- Once it is established that a vulnerability exists or you 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.

Security researchers are expected to uphold the following principles in their activities:

- Avoid intentionally accessing the content of any communications, data, or information transiting or stored on USAID information systems, except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- Do no harm and will not exploit any vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability.
- Do not delete, alter, share, retain, or destroy USAID data, or render USAID data inaccessible; do not intentionally access any personally identifiable information; and do not disclose any personally identifiable information inadvertently encountered to a third party.
- Make every effort to avoid access to personally identifiable information and 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.
- Do not submit a high volume of low-quality reports.

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; and
- Testing any system other than the systems set forth in the 'Scope' section above.

Reporting a Vulnerability

USAID accepts vulnerability reports via electronic mail to vdp@usaid.gov. Reports may be submitted anonymously. However, if you share contact information, we will acknowledge receipt of your report within five (5) business days. We may also 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, your report may be shared with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under their coordinated vulnerability disclosure process, as well as any affected vendors. USAID 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 USAID would like to see from you

In order to help USAID triage and prioritize submissions, recommendations for the content of your report submission are listed below:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Describe 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 USAID

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

- Within five (5) business days, USAID will acknowledge that your report has been received.
- To the best of our ability, USAID 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.
- USAID 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.

VDP Reward

There will be no reward or bounty for the submitted report. Submissions to VDP helps USAID achieve the goal to "promote good faith security research, ultimately resulting in improved security and coordinated disclosure across the federal civilian enterprise." USAID appreciates and encourages any notifications on vulnerabilities so we may better protect our environment.

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
1.1	May 27, 2021	Scope change and minor updates
1.2	August 27, 2021	Scope change

1.3	October 1, 2021	Scope change
1.4	December 1, 2021	Scope change
1.5	January 3, 2022	Scope change
1.6	March 1, 2022	Scope change
1.7	May 2, 2022	Scope clean up & scope additions
1.8	June 3, 2022	Scope change
1.9	October 14, 2022	Scope change
1.10	August 10, 2023	Scope Change and Minor Updates
1.11	September 25, 2023	Scope change
1.12	February 5, 2024	Scope change
1.13	May 6, 2024	Scope change