The Department of Housing and Urban Development

Vulnerability Disclosure Policy

HUD Handbook 2400.45 REV 2.0

6/21/2023

DOCUMENT CHANGE HISTORY

Issue	Date	Pages Affected	Description
Revision 1.0	March 1, 2021	All	Final Version 1.0
Revision 2.0	August 26, 2022	1, 21, A1	Included all systems within scope
Revision 2.1	March 24, 2023	3	Update links

TABLE OF CONTENTS

1 Introduction

Maintaining the security of U.S. Department of Housing and Urban Development (HUD) networks is a high priority at HUD. Information technologies provide critical services to housing beneficiaries, their families, and HUD employees and contractors. Ultimately, HUD data security ensures that HUD's mission is accomplished to create strong, sustainable, inclusive communities while developing quality affordable homes for all.

The cybersecurity researcher community regularly makes valuable contributions to the security of organizations and the broader Internet. If you have information about a vulnerability in a HUD website or web application, HUD wants to hear from you.

Information submitted to HUD under this policy will be used to mitigate or remediate vulnerabilities in HUD networks or applications.

2 Purpose

The Vulnerability Disclosure Policy (VDP) is intended to give security researchers clear guidelines for conducting vulnerability discovery activities, what systems and types of research are covered under this policy, how to send vulnerability reports, and how long HUD asks security researchers to wait before publicly disclosing vulnerabilities.

3 Rescission

This policy is new and rescinds Revision 1.0 of the Vulnerability Disclosure Policy. If manuals, memorandums, or guidance documents were published by HUD before this policy conflict, this policy shall take precedence.

4 Scope

This policy applies to the members of the public conducting vulnerability discovery activities. The policy does not apply to HUD employees and contractors with HUD network access, who should follow the HUD Departmental Rules of Behavior (RoB) and coordinate vulnerability discovery activities with HUD OCIO.

This policy applies to all HUD **Error! Reference source not found.**systems and services. Additionally, vulnerabilities found in systems from HUD 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 HUD at VDP@hud.gov before starting your research (or the security contact for the system's domain name listed in the .gov WHOIS).

Though HUD develops and maintains other internet-accessible systems or services, active research and testing should only be conducted on the systems and services covered by the scope of this document.

5 Effective Implementation Date

This policy is effective immediately upon the date of approval.

6 Policy

If you make a good faith effort to comply with this policy during your security research, HUD will consider your research to be authorized, will work with you to understand, and resolve the issue quickly, and 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, HUD will make this authorization known.

6.1 How to Submit a Report

Please email a detailed summary of the vulnerability to VDP@hud.gov. In order to help triage and prioritize submissions, HUD recommends that your reports include:

- Uniform Resource Locator (URL)
- Type of issue
- Product version, and configuration of software containing the bug
- Step-by-step instructions to reproduce the issue (including technical details)
- Any available proof of concept code
- Potential Impact of the issue
- Suggested mitigation or remediation actions, as appropriate
- What tool(s), if any, were utilized to detect the issue

To assist in the reporting, a template is provided in Appendix A:. This template is to aid in reporting and is not required. Reports may be submitted anonymously. If you share contact information, HUD will acknowledge receipt of your report within three (3) business days as described in Section 7, What you Can Expect From Us.

6.2 Guidelines and Test Methods

HUD will operate in good faith with researchers who discover, test, and submit vulnerabilities or indicators of vulnerabilities in accordance with these guidelines:

- Your activities are limited exclusively to –
    - (1) Testing to detect a vulnerability or identify an indicator related to a vulnerability; or

  - (2) Sharing with, or receiving from, HUD information about a vulnerability or an indicator related to a vulnerability.
- You do no harm and do 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.
- You avoid intentionally accessing the content of any communications, data, or information transiting or stored on HUD information system(s) – except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- You do not copy and transfer (exfiltrate) any data from systems under any circumstances.
- You do not intentionally compromise the privacy or safety of HUD personnel (e.g. contractors or affiliates), or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any HUD personnel or entities, or any third parties.
- You do not publicly disclose any details of the vulnerability, indicator of vulnerability, or the content of information rendered available by a vulnerability, except upon receiving explicit written authorization from HUD.
- You do not conduct denial of service testing.
- You do not conduct any form (electronic, manual, automated, etc.) of testing during the first ten (10) business days of every month of the following sites:
  - www.ginniemae.gov
  - https://bulk.ginniemae.gov/
  - https://tst.ginniemae.gov/pages/default.aspx
  - https://my.ginniemae.gov/webcenter/portal/public?_afrLoop=2205282976811924
- You do not conduct social engineering, including spear phishing, of HUD personnel or contractors.
- You do not submit a high-volume of low-quality reports.

If at any point you are uncertain whether to continue testing, contact VDP@hud.gov.

6.3 Legal

You must comply with all applicable Federal, State, and local laws in connection with your security research activities or other participation in this vulnerability disclosure program.

HUD does not authorize, permit, or otherwise allow (expressly or impliedly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law.

If you conduct your security research and vulnerability disclosure activities in accordance with the restrictions and guidelines set forth in this policy:

(1) HUD will not recommend or pursue any law enforcement or civil lawsuits related to such activities, and

“(2) 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 we will work with you to understand and resolve the issue quickly. HUD 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, this authorization will be available for disclosure.

To the extent that any security research or vulnerability disclosure activity involves the networks, systems, information, applications, products, or services of a non-HUD entity (e.g., other Federal departments or agencies; State, local, or tribal governments; private sector companies or persons; employees or personnel of any such entities; or any other such third party), that non-HUD third party may independently determine whether to pursue legal action or remedies related to such activities.

HUD may modify the terms of this policy at any time.

7 What you Can Expect From Us

HUD OCIO takes every disclosure seriously and appreciates the efforts of security researchers. HUD OCIO will investigate every disclosure and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.

HUD has a unique information and communications technology which routinely handles housing and financial information. Many HUD technologies are involved in critical housing decisions and could have impact on the federal government, state governments, local communities, and individual beneficiaries. HUD must take extra care while investigating the impact of vulnerabilities and providing a fix.

HUD remains committed to coordinating with the researcher as openly and quickly as possible. This includes:

- Within three (3) business days, HUD will acknowledge receipt of your report. HUD’s security team will investigate the report and may contact you for further information.
- As appropriate and to the best of our ability, HUD will confirm the existence of the vulnerability to the researcher and keep the researcher informed as remediation of the vulnerability is underway.

- HUD will maintain an open dialogue to discuss issues.
- HUD wants researchers to be recognized publicly for their contributions if that is the researcher's desire. HUD will seek to allow researchers to be publicly recognized whenever possible if the researcher(s) choose to. HUD will work with researchers to set a reasonable time period between when a vulnerability is reported and when it is publicly disclosed.

Information submitted to HUD under this policy will be used to mitigate or remediate reported vulnerabilities in HUD networks or applications, or the applications of HUD vendors. HUD may share your vulnerability reports 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 or open-source projects. HUD will not share your name or contact information without express permission or as otherwise required by law.

8 Definitions

This section includes definitions associated with the terms within this policy.

Table 1: Definitions

Word	Definitions
Good Faith	Good faith security research means accessing a computer or software solely for purpose of testing or investigating a security flaw or vulnerability and disclosing those findings in alignment with the VDP.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.
Network	A system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Disclosure	The act of initially providing vulnerability information to a party that was not believed to be previously aware.

9 Authorities and References

HUD has established this policy based on:

- Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020 https://cyber.dhs.gov/bod/20-01/
- U.S. Department of Justice, *A Framework for a Vulnerability Disclosure Program for Online Systems*, v1.0, July 2017 https://www.justice.gov/criminal-ccips/page/file/983996/download
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*, October 2018 https://www.iso.org/standard/72311.html
- CISA Coordinated Vulnerability Disclosures (CVD) Process, https://www.cisa.gov/coordinated-vulnerability-disclosure-process

10 Glossary – Abbreviations and Acronyms

This section lists abbreviations and acronyms as annotated in the policy.

Acronym	Definition
BOD	Binding Operational Directive
CISA	Cybersecurity and Infrastructure Security Agency
CVD	Coordinated Vulnerability Disclosures
HUD	Department of Housing and Urban Development
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OCIO	Office of the Chief Information Officer
RoB	Rules of Behavior
URL	Uniform Resource Locator
VDP	Vulnerability Disclosure Policy

Appendix A: Vulnerability Disclosure Template

URL	
Type of Issue	
Description of Vulnerability	
Potential Impact	
Impacted Product	*e.g., product, version, and configuration of any software or hardware potentially impacted*

Step-by-Step Reproduction Instructions (including technical details)**:**
Proof of Concept Code (if available):
Suggested Mitigation or Remediation Actions (as appropriate):
What tool(s), if any, were utilized to detect the issue:

I would like to be contacted regarding this issue:
☐Yes ☐No

If yes, please provide contact information:

Name	
Email	
Phone	