



**Homeland
Security**

Vulnerability Disclosure Program (VDP) Policy and Rules of Engagement (ROE)

Version 1.4
December 22, 2022

Protecting the Information that Secures the Homeland

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	March 19, 2019	Initial draft
1.1	May 6, 2019	Revision of Initial draft
1.2	February 1, 2021	Revised draft per CISA guidance
1.3	February 9, 2021	Revised per CISO and DOJ
1.4	December 22, 2022	Revised scope per CISA & OGC

C O N T E N T S

1.0 PURPOSE.....1

2.0 OVERVIEW1

3.0 SCOPE1

4.0 HOW TO SUBMIT A REPORT2

5.0 GUIDELINES2

6.0 PARTICIPANT EXPECTATIONS2

7.0 LEGAL / AUTHORIZATION.....4

1.0 PURPOSE

In accordance with Section 101 and Title I of the SECURE Technology Act (P.L. 115-390), this policy provides security researchers with clear guidelines for (1) conducting vulnerability and attack vector discovery activities directed at Department of Homeland Security (DHS) systems and (2) submitting those discovered vulnerabilities. This policy has been developed in consultation with the Attorney General, the Secretary of Defense, the Administrator of GSA, and non-governmental security researchers.

2.0 OVERVIEW

DHS has a unique information and communications technology footprint that is tightly interwoven and globally deployed. Many DHS technologies are deployed in critical infrastructure systems and, to varying degrees, support ongoing homeland security operations; the proper functioning of DHS systems and applications can have a life-or-death impact on DHS personnel and international allies and partners of the United States.

Our information systems provide critical services in support of the widespread, critical missions of DHS. Maintaining the security of our networks is a high priority at DHS. Ultimately, our network security ensures that we can accomplish our missions and contribute to the success of the individuals who contribute to the mission success.

DHS recognizes that security researchers regularly contribute to the work of securing organizations and the Internet as a whole. Therefore, DHS invites reports of any vulnerabilities discovered on internet-accessible DHS information systems, applications, and websites¹. Information submitted to DHS under this policy will be used for defensive purposes – to mitigate or remediate vulnerabilities in our networks. This program upholds the DHS motto “See Something – Say Something” in the virtual environment by positively engaging with and establishing a communication loop between researchers and DHS.

Hereinafter, researcher² may be referred to as “you” or “your” and DHS may be interchangeably used in conjunction with or alternatively referenced as “we”, “our”, or “us”.

3.0 SCOPE

This policy applies to any internet-accessible information system, application, or website owned, operated, or controlled by DHS, including any web or mobile applications hosted on those sites¹. Contractor information systems operated on behalf of DHS are not included within the scope of this policy.

¹ These websites constitute “information systems” as defined by 44 U.S.C. 3502.

² The term “Researcher” in this document is intended to be consistent with the terms “Finder” and/or “Reporter” as used in ISO/IEC 29147:2014(E) and the CERT® Guide to Coordinated Vulnerability Disclosure, and may be substituted with “you, your”.

This policy applies to all domains and subdomains listed at the below link which are listed as belonging to the Department of Homeland Security (DHS):

<https://github.com/cisagov/dotgov-data/blob/main/current-federal.csv>

4.0 HOW TO SUBMIT A REPORT

Please submit a report of the vulnerability at <https://www.dhs.gov/topic/cybersecurity>. An example of the vulnerability report would include a detailed summary, including:

- Type of vulnerability
- IP Address or hostname
- Description of vulnerability
- Instructions to replicate
- Potential impact to system/site
- Recommended remediation actions

5.0 GUIDELINES

You **MUST** read and agree to abide by the guidelines in this policy for conducting security research and disclosure of vulnerabilities or indicators of vulnerabilities related to DHS information systems. We will presume you are acting in good faith when you discover, test, and submit reports of vulnerabilities³ or indicators of vulnerabilities in accordance with these guidelines:

- You **MAY**⁴ test internet-accessible DHS information systems to detect a vulnerability or identify an indicator related to a vulnerability for the sole purpose of providing DHS information about such vulnerability.
- You **MUST** avoid harm to DHS information systems and operations.
- You **MUST NOT** exploit any vulnerability beyond the minimal amount of testing required to prove that the vulnerability exists or to identify an indicator related to that vulnerability.
- You **MUST NOT** intentionally access the content of any communications, data, or information transiting or stored on DHS information system(s) – except to the

³ Vulnerabilities throughout this policy may be considered “security vulnerabilities” as defined by Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, § 102 : “The term “security vulnerability” means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.”

⁴ The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.

- You MUST NOT exfiltrate any data under any circumstances.
- You MUST NOT intentionally compromise the privacy or safety of DHS personnel (e.g., civilian employees) or any legitimate third parties.
- You MUST NOT intentionally compromise the intellectual property or other commercial or financial interests of any DHS personnel or entities or any legitimate third parties.
- You MUST NOT disclose any details of any extant DHS information system vulnerability or indicator of vulnerability to any party not already aware at the time the report is submitted to DHS.
- In the event that you find a vulnerability in a DHS information system consequent to a vulnerability in a generally available product, you MAY report the product vulnerability to the affected vendor or a third party vulnerability coordination service in order to enable the product to be fixed.
- You MAY disclose to the public the prior existence of vulnerabilities already fixed by DHS, potentially including details of the vulnerability, indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability. If you choose to disclose, you should do so in consultation with DHS.
- You MUST NOT disclose any incidental proprietary data revealed during testing or the content of information rendered available by the vulnerability to any party not already aware at the time the report is submitted to DHS.
- You MUST NOT cause a denial of any legitimate services in the course of your testing.
- You MUST NOT conduct social engineering in any form of DHS personnel or contractors.
- You SHOULD strive to submit high-quality reports.
- You MUST NOT submit a high-volume of low-quality reports.
- You MUST comply with all applicable Federal, State, and local laws in connection with security research activities or other participation in this vulnerability disclosure program.

If at any point you are uncertain of whether to proceed with testing, please contact our team at Vulnerability.Disclosure.Prog@hq.dhs.gov.

6.0 PARTICIPANT EXPECTATIONS

We take every disclosure seriously, and very much appreciate your efforts. We are committed to coordinating with you as openly and expeditiously as possible. The

contents of information provided in the reports and follow-up communications are processed and stored on a U.S. Government information system. You can expect us to do the following:

- We SHALL investigate every reported vulnerability and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.
- If you opt to provide your contact information, our security team MAY contact you for further information.
- We SHALL, to the best of our ability, validate the existence of the vulnerability.
- We MAY disclose to the public the prior existence of vulnerabilities remedied by us, potentially including details of the vulnerability such as the indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability.
- In the event that we choose to publicly disclose your reported vulnerability we SHALL recognize your contribution as it must pertain to improving our security, the first to report a unique vulnerability, and if your report triggers a code or configuration change.
- In the event you report a vulnerability pertaining to a generally available product, we SHALL validate the vulnerability pertaining to the identified product is legitimate and that it is a product used within our environment. After those factors are verified, we MAY report the product vulnerability to the affected vendor or to a third-party vulnerability coordination service.
- We SHALL NOT forward your name and contact information to any affected vendors unless otherwise requested by you.
- We MAY NOT disclose information provided by any vendor unless the vendor explicitly states to do so.
- We SHALL request 30 days for acknowledgement and 90 days for mitigation development, and deployment.
- We MAY consult with you and any affected vendors to determine our public disclosure⁵ plans of the vulnerability
- In cases where a product is affected and the vendor is unresponsive, or fails to establish a reasonable timeframe for remediation, we MAY disclose product vulnerabilities 45 days after the initial contact is made, regardless of the existence or availability of patches or workarounds from affected vendors.

⁵ “Public disclosure” means the release of previously undisclosed information related to a vulnerability by DHS, a vendor, or a researcher to [the public/non-governmental persons or entities] through mediums that include, but are not limited to, official press releases, blogs, social media platforms, email, or other webpages. We SHALL make our disclosure determinations based on relevant factors, such as: whether the vulnerability has already been publicly disclosed, the severity of the vulnerability, potential impact to critical infrastructure, possible threat to public health and safety, immediate mitigations available, vendor responsiveness and feasibility for creating an upgrade or patch, and vendor estimate of time required for customers to obtain, test, and apply the patch. Active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure.

7.0 LEGAL / AUTHORIZATION

If you make a good faith effort to conduct your research and disclose vulnerabilities in accordance with the guidelines set forth in this policy, (1) DHS will not recommend or pursue any law enforcement or civil lawsuits related to such activities, and (2) in the event of any law enforcement or civil action brought by any entity other than DHS, DHS will affirm that your research and disclosure activities were conducted pursuant to, and in compliance with, this policy. This agreement is effective at the time of the form submission on the DHS.gov webpage.

Please note that individuals and entities that conduct activities as authorized by this policy and comply with its terms will receive legal protection from criminal or civil liability under section 1030 of title 18, United States Code, and similar laws penalizing unauthorized access to computers.

DHS does not authorize, permit, or otherwise allow (expressly or implicitly) 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. Any activities that are inconsistent with this policy or the law may lead to criminal and/or civil liabilities. Third parties (e.g., any non-DHS entity) may independently determine whether to pursue legal recourse or related.

DHS may modify the terms of this policy, or suspend this policy at any time.
