U.S. Customs and Border Protection

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

Version 1.0

June 22, 2022

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	June 6, 2022	Initial draft
1.0	June 16, 2022	Office of Chief Counsel Revision
1.0	June 22, 2022	Office of Chief Counsel Approval

CONTENTS

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 U.S. Customs and Border Protection (CBP) systems and (2) submitting those discovered vulnerabilities. This policy is in accordance with Department of Homeland Security (DHS) policy[1] that was developed by DHS and the DHS Cybersecurity & Infrastructure Security Agency (CISA), in consultation with the Attorney General, the Secretary of Defense, the Administrator of GSA, and non-governmental security researchers.

2.0 OVERVIEW

As a component of DHS, CBP has an information and communications technology footprint that is tightly interwoven and globally deployed. Many DHS/CBP technologies are deployed in critical infrastructure systems and, to varying degrees, support ongoing homeland security operations.

CBP's information systems provide essential services in support of our mission to protect the American people, safeguard our borders, and enhance the nation's economic prosperity. To carry out this mission, we are committed to diligently maintaining the security of our information systems.

CBP recognizes that security researchers regularly contribute to the work of securing organizations and the internet. Therefore, CBP invites reports of any vulnerabilities discovered on internet-accessible CBP information systems, applications, and websites.[2] Information submitted to CBP under this policy will be used for defensive purposes, that is, 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 CBP.

Hereinafter, researcher[3] may be referred to as "you" or "your" and CBP 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 CBP, including any web or mobile applications hosted on those sites. Contractor information systems operated on behalf of CBP are not included within the scope of this policy.

[1] https://www.dhs.gov/sites/default/files/publications/21_0216_vdp-policy-roe-approved.txt.
[2] These websites constitute "information systems" as defined by 44 U.S.C. 3502(8).
[3] 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 the following systems and services:

- *CBP.gov[α]
- Including all CBP publicly owned non-CBP.gov domains

4.0 HOW TO SUBMIT A REPORT

Reports of vulnerabilities may be submitted at https://www.cbp.gov/topic/cybersecurity. This website contains more detailed, step-by-step instructions on how to submit a vulnerability report. By submitting a report, you acknowledge that you have no expectation of payment from the U.S. Government. If you are a duly authorized researcher taking part in a CBP Bug Bounty engagement, the payment terms and conditions of your engagement apply. In all cases, you expressly waive any future pay claims against the U.S. Government related to your submission.

An example of the vulnerability report would include a detailed summary which identifies:

- Type of vulnerability.
- IP address or hostname.
- Description of vulnerability.
- Instructions to replicate.
- Potential impact to system/site; and
- Recommended remediation actions.

5.0 GUIDELINES

You MUST[4] read and agree to abide by the guidelines in this policy for conducting security research and disclosure of vulnerabilities[5] or indicators of vulnerabilities related to CBP information systems. We will presume you are acting in good faith when you discover, test, and submit reports of vulnerabilities or indicators of vulnerabilities in accordance with these guidelines:

- You MAY test internet accessible CBP information systems to detect a vulnerability or identify an indicator related to a vulnerability for the sole purpose of providing CBP information about such vulnerability.
- You MUST avoid harm to CBP 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 MAY anonymously submit vulnerability reports.

[α] the "*CBP.gov" refers to any domain ending in CBP.gov.

[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 the Internet Engineering Task Force RFC 2119 (defining key words for the Best Current Practices for the Internet Community).

[5] 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."

- You MUST NOT intentionally access the content of any communications, data, or information transiting or stored on CBP 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 MUST NOT exfiltrate any data under any circumstances.
- You MUST NOT intentionally compromise the privacy or safety of CBP 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 CBP personnel or entities or any legitimate third parties.
- You MUST NOT disclose any details of any extant CBP information system vulnerability or indicator of vulnerability to any party not already aware at the time the report is submitted to CBP.
- If you find a vulnerability in a CBP 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 CBP, 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 MUST do so in consultation with CBP.
- 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 CBP.
- You MUST NOT cause a denial of any legitimate services in the course of your testing.
    - 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
- You MUST NOT conduct social engineering in any form of CBP 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.

Once you have 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.

If at any point you are uncertain of whether to proceed with testing, please contact our team at CBPVULNERABILITYDISCLOSURE@cbp.dhs.gov.

6.0 PARTICIPANT EXPECTATIONS

We take every disclosure seriously, and very much appreciate your participation. 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. CBP endeavors to do the following:

- We will strive to 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.
- To the best of our ability, we will validate the existence of the vulnerability.
- We may disclose[6] 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 will publicly reference you and credit your contribution if the following conditions are met: (i) the vulnerability pertained to improving our security; (ii) you were the first to report the vulnerability; (iii) you reported a unique vulnerability; and (iv) your report triggered a code or configuration change.
- In the event you report a vulnerability pertaining to a generally available product, we intend to 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 will endeavor to not forward name and contact information to any affected vendors unless otherwise requested by you.
- Unless required or otherwise permitted by federal law, we may not disclose confidential information provided to CBP by a vendor in connection with a vulnerability report unless the vendor explicitly states to do so.

[6] "Public disclosure" means the release of previously undisclosed information related to a vulnerability by CBP, 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.

- We request 30 days for acknowledgement of any reported vulnerability and 90 days for mitigation development, and deployment after CBP acknowledgment.
- We may consult with you if you provide your contact information, and any affected vendors to determine our public disclosure 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.

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) CBP 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 CBP, CBP will affirm that your research and disclosure activities were conducted pursuant to, and in compliance with, this policy.

CBP 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-CBP entity) may independently determine whether to pursue legal recourse.

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