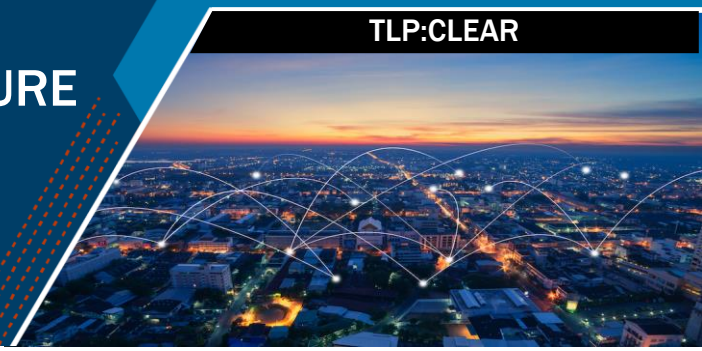
VULNERABILITY DISCLOSURE POLICY (VDP) PLATFORM FACT SHEET



OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) established the Vulnerability Disclosure Policy (VDP) Platform to improve the security of federal civilian executive branch (FCEB) agencies' internet-accessible systems through a centrally managed vulnerability intake system. The VDP Platform gives participating agencies increased access to a global community of public security researchers and streamlines the vulnerability management process. The VDP Platform was launched in July 2021 and has since furthered:

- Binding Operational Directive (BOD) 20-01, which requires agencies to develop and publish a VDP,
- BOD 22-01, which focuses on reducing the risk of known exploited vulnerabilities (KEVs), and
- Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," which seeks to improve agencies' vulnerability management capabilities, among other goals.

FEATURES

CISA's VDP Platform provides a primary entry point for public security researchers and alerts participating agencies to potential issues with their assets. At a high level, the service:

- Screens spam and performs base-level validation on submitted reports.
- Assigns initial prioritization ratings to valid reports.
- Escalates vulnerability reports that require agency attention.
- Provides data insight into trends in vulnerability types, criticality of reports, top public security researchers, etc.
- Provides a web-based communication mechanism between researcher and agency.
- Enables users to create and manage role-based accounts for their organization and suborganizations.
- Offers an application programming interface (API) to facilitate actions on vulnerability reports, such as pulling reports into agency ticketing systems.
- Automatically generates agency's quarterly BOD 20-01 metrics.
- Includes optional functionality for agencies interested in conducting bug bounties, which are events designed to provide financial incentives to researchers.

VALUE

CISA's VDP Platform offers agencies several benefits, including:

- **Compliance With Federal Requirements:** CISA centrally manages the VDP Platform, ensuring that the service meets relevant government-wide standards, policies, and requirements.
- **Minimal Cost:** CISA is utilizing a shared service approach to deliver the VDP Platform to participating agencies, centralizing the administrative costs of the service. The VDP Platform is CISA-funded through February 2025.
- **Reduced Agency Burden:** CISA hosts the VDP Platform, manages administrative responsibilities, and provides user management and support. The service includes initial triaging related to validity of reports submitted, which assists with timely validation of reports.
- **Improved Information Sharing Across Federal Civilian Enterprise:** The VDP Platform improves information sharing across the federal civilian enterprise by enabling CISA to maintain insight into disclosure activities.
- **Automated Known Exploited Vulnerabilities (KEV) Support:** The VDP Platform facilitates agency compliance with BOD 22-01 by providing automated support to help agencies match vulnerability submissions with KEVs (present in CISA's KEV Catalog).

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

- **Centralized Access Point for Researchers:** Participating agencies can choose to host their VDP on the platform, generating increased visibility and researcher engagement.
- **Automated Metrics and Reports:** The VDP Platform automatically generates the following reporting metrics to satisfy BOD 20-01 requirements:
    - Number of valid reports
    - Number of currently open and valid reported vulnerabilities
    - Median age of open and valid reported vulnerabilities
    - Median age of reports older than 90 days
    - Number of currently open and valid vulnerabilities older than 90 days from report receipt
    - Number of all reports older than 90 days, sorted by risk/priority level
    - Time needed to validate and mitigate submitted vulnerabilities and reports
    - Time needed to initially respond to the researcher

ROLES AND RESPONSIBILITIES

CISA's VDP Platform is a software-as-a-service application, designed to alert participating agencies about issues on their internet-accessible systems. However, vulnerability remediation on federal information systems remains the responsibility of the agencies operating those networks. A breakdown of roles is as follows:

- **Public Security Researchers:** Utilize the VDP Platform as a central place to access participating agency VDPs and to report vulnerabilities in systems of participating agencies.
- **Platform Vendor (EnDyna/Bugcrowd):** Provide screening, initial validation, and prioritization on all incoming vulnerability reports.
- **CISA:** Maintain insight into disclosure activities, provide vendor oversight and training on the VDP Platform, and assist with troubleshooting any platform issues.
- **User Agency:** Maintain agency-specific program within the VDP Platform, validate triaged reports and work to remediate valid findings.

SIGN UP

The VDP Platform is available to all FCEB agencies that fall under CISA's authorities. Any agency interested in participating or receiving more information on the VDP Platform, or other cybersecurity shared services, can reach out to CyberSharedServices@cisa.dhs.gov.