Vulnerability Disclosure Policy Platform

November 2021

The Cybersecurity and Infrastructure Security Agency's (CISA) Vulnerability Disclosure Policy (VDP) Platform supports agencies with the option to use a centrally managed system to intake vulnerability information from the public to improve the security of the agency's internet-accessible systems. In support of CISA's Binding Operational Directive (BOD) 20-01, Develop and Publish a Vulnerability Disclosure Policy, the VDP Platform aims to promote good faith security research, ultimately resulting in improved security and coordinated disclosure across the federal civilian enterprise.

BENEFITS

CISA's VDP Platform provides participating agencies with the following benefits:

- **Minimal Cost.** By using a shared service approach to deliver the VDP Platform to participating agencies, CISA has centralized the administrative costs of the service. Additionally, CISA will cover all fixed costs directly associated with the VDP Platform throughout the lifecycle of the contract, including costs associated with a set number of triaged reports per agency beginning Fiscal Year (FY) 2021 through January 2023.
- **Binding Operational Directive 20-01 Reporting.** The VDP Platform automatically facilitates the majority of required compliance reporting metrics to CISA on behalf of the participating agencies, reducing agency reporting efforts.
- **Reduced Agency Burden.** The VDP Platform solution provider hosts and manages the VDP Platform, including administrative responsibilities, user management, and Platform support. CISA oversees the system's security and compliance with federal regulations. The service includes basic assessment of submitted vulnerability reports, enabling agencies to focus on reports that impact their agency environments.
- **Improved Information Sharing Across Federal Enterprise.** By allowing CISA to maintain insight into disclosure activities, the VDP Platform increases the sharing of vulnerability information.

FUNCTIONALITY HIGHLIGHTS

The VDP Platform uses the functionality highlighted below to provide a primary point of entry for vulnerability reporters to alert participating agencies of potential issues on federal information systems:

Screening. The service screens spam and performs a base level of validation on submitted reports.

Data Insights. CISA will use data collected from the service to track reported vulnerabilities and link related reports by vulnerability type, or for other purposes, including meeting the BOD 20-01 reporting requirements.

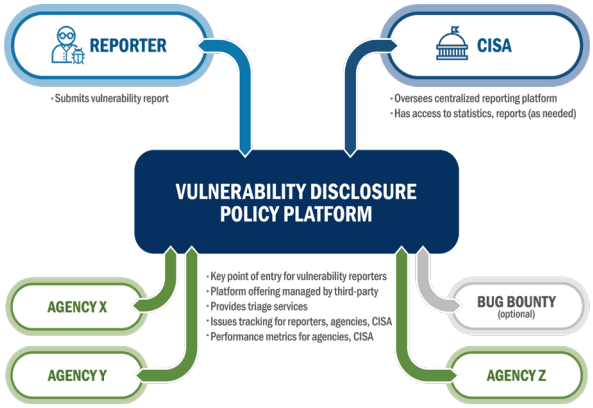
Communication. The Platform provides a web-based communication mechanism between vulnerability reporter and the agency and allows agency users to create and manage role-based accounts for their organization.

Application Programming Interface (API). The Platform's API executes various actions, such as pulling reports into agency ticketing systems and providing alerts to the reporter, CISA, and agency users based on events of interest, metrics, defined thresholds, etc.

HOW IT WORKS

The VDP Platform is a software-as-a-service application that serves as a primary point of entry for vulnerability reporters to alert participating agencies to issues on their internet accessible systems. The remediation of identified vulnerabilities on federal information systems remains the responsibility of the agencies operating the impacted systems.

Vulnerability reporters from the public submit reports on vulnerabilities found within the systems of participating agencies to the centralized VDP Platform. Once reports are received, the VDP Platform solution provider screens and triages the submissions, validating reports that appear to be legitimate. Agency users have access to the Platform by logging into the VDP Platform interface, viewing the agency dashboard that lists vulnerability submissions and general statistics. CISA has read-only access to all agency reports to view aggregated statistical data, maintaining insight into the disclosed activities but not actively participating in each remediation process.



CUSTOMIZATION

Participating agencies can leverage the VDP Platform through three customizable approaches:

1. **Host on VDP Platform Solution Provider's Website.** Vulnerability reporters visit the solution provider's website to disclose identified vulnerabilities.

2. **Host Embedded Form on Agency's Website.** Vulnerability reporters visit the associated agency's VDP page and fill out an embedded form, which is then automatically routed to the VDP Platform for triaging.

3. **Host Agency's VDP Policy on Both Solution Provider's Website and on Agency's Website**: Vulnerability reporters can disclose vulnerabilities through either mechanism, maximizing visibility of the policy while avoiding redirecting researchers to the solution provider's website from a government website.

HOW CAN YOU REQUEST SERVICES?

Any agency interested in participating or receiving additional information should contact CISA's Cyber Quality Service Management Office (QSMO) at QSMO@cisa.dhs.gov and provide contact information and the agency system(s) in scope for the VDP Platform.

ABOUT THE CYBER QSMO

CISA's Cyber Quality Service Management Office (QSMO) is the single shared service office for managing cybersecurity solutions for the Federal Civilian Executive Branch (FCEB). CISA's Cyber QSMO centralizes, standardizes, automates, and offers high-quality, cost-effective cybersecurity services and products on the Cyber QSMO Marketplace, providing federal civilian departments and agencies with a one stop-shop for cybersecurity services. As part of our end-to-end service management model, we are committed to providing integration and adoption support to our customers through a unified shared services platform.

OUR CYBERSECURITY MARKETPLACE

With initial launch in Fall 2020, CISA's Cyber QSMO Marketplace is an online storefront for high-quality and cost-effective cybersecurity services. CISA's Cyber QSMO's Marketplace offers best-in-class cybersecurity services from CISA, federal, and, eventually, commercial service providers. These CISA-validated services and provider partnerships will evolve and expand as the QSMO matures. By offering CISA-validated cybersecurity services, the Cyber QSMO Marketplace reduces purchasing agencies' burden of having to conduct their own research in order to vet and acquire affordable cyber services that comply with federal requirements and standards.