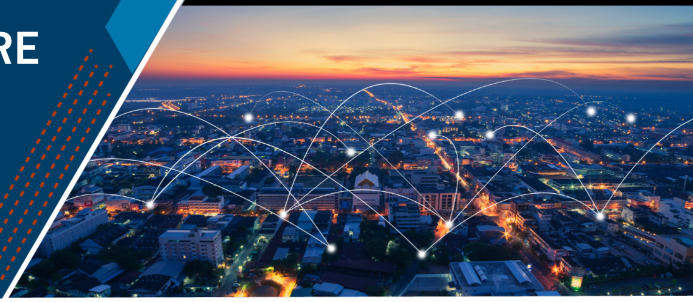
VULNERABILITY DISCLOSURE POLICY (VDP) PLATFORM FREQUENTLY ASKED QUESTIONS



WHAT IS THE VDP PLATFORM?

The Vulnerability Disclosure Policy (VDP) Platform is a centrally managed software-as-a-service (SaaS) system that intakes vulnerability information from — and enables collaboration with — the public security researcher community to improve agency cybersecurity. In furtherance of binding operational directive (BODs) 20-01 and 22-01 issued by the Cybersecurity and Infrastructure Security Agency (CISA), the VDP Platform aims to promote good faith security research, ultimately resulting in improved security and coordinated disclosure across the federal civilian executive branch (FCEB).

CISA manages the VDP Platform, ensuring that the service meets relevant government-wide standards, policies, and requirements.

ARE THERE COSTS OR FEES ASSOCIATED WITH THE VDP PLATFORM?

The VDP Platform is centrally funded by CISA and the agency intends to maintain this funding model

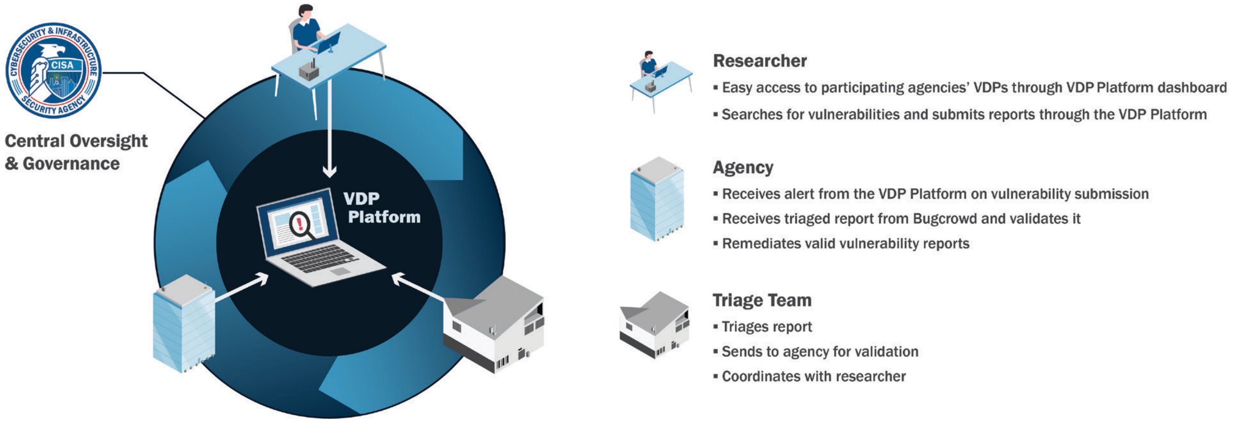
WHY SHOULD AGENCIES USE THE VDP PLATFORM?

The VDP Platform offers agencies several benefits, including:

1. **Screening and Validation:** The service screens spam and performs a base-level validation and prioritization on all submitted reports.
2. **Data Insights:** The VDP Platform provides data insight into reports, identifying vulnerability trends, top researchers, and more. The service includes data insights on submitted vulnerability reports, enabling agencies to prioritize remediation of the most impactful reports.
3. **Communication:** The VDP Platform provides a web-based communication mechanism between the researcher and the agency, allowing agency users to create and manage role-based accounts for their organization.
4. **Application Programming Interface (API):** The VDP Platform's API equips agencies with the ability to pull reports into existing agency ticketing systems. Agencies can customize alerts/notifications based on events of interest, metrics, defined thresholds, and more.
5. **BOD 20-01 Reporting:** The service automatically generates reporting metrics to satisfy BOD 20-01's requirements.
6. **BOD 22-01 Compliance:** The VDP Platform provides support to help agencies identify which submissions match vulnerabilities present within CISA's Known Exploited Vulnerabilities (KEV) Catalog.
7. **Bug Bounty:** Bug bounty programs offer financial incentives to researchers searching for vulnerabilities. The VDP Platform provides support to an agency's bug bounty effort. Establishing a bug bounty program is an optional feature of the VDP Platform and is not required by BOD 20-01. CISA will provide guidance on how to maximize the impact of a potential bug bounty program, while agencies determine authority, readiness, scope, and duration. Agencies are responsible for providing the funding for the researcher payout portion of a bug bounty event.

8. **Improved Information Sharing Across Federal Enterprise:** The VDP Platform plays a crucial role in facilitating threat information sharing between researchers, federal agencies, and CISA. The platform provides a secure method for researchers to submit discovered vulnerabilities, reducing the risk of unauthorized disclosures. Through the information sharing, federal agencies can collaborate with researchers to identify and remediate potential vulnerabilities. As vulnerabilities are disclosed, the shared information contributes to a broader understanding of emerging threats.

WHAT ARE RESPONSIBILITIES OF AGENCIES, RESEARCHERS, THE VENDOR, AND CISA?



Researcher
- Easy access to participating agencies' VDPs through VDP Platform dashboard
- Searches for vulnerabilities and submits reports through the VDP Platform

Agency
- Receives alert from the VDP Platform on vulnerability submission
- Receives triaged report from Bugcrowd and validates it
- Remediates valid vulnerability reports

Triage Team
- Triages report
- Sends to agency for validation
- Coordinates with researcher

Figure 1: VDP Platform responsibilities and actions for agencies, researchers, vendor, and CISA

ARE VULNERABILITY REPORTS VISIBLE FOR ALL AGENCIES TO VIEW?

No, agencies can only see the reports for their specific instance on the VDP platform.

HOW ARE VULNERABILITIES PRIORITIZED?

The triaging team utilizes Bugcrowd's Vulnerability Rating Taxonomy (VRT). The Bugcrowd VRT is an open-source, industry-standard taxonomy that aligns customers and researchers on a common set of risk priority ratings for common vulnerabilities and edge cases. It's important to recognize that base priority does not equate to "industry accepted impact." As agencies assess the severity of their vulnerability reports, it is recommended to utilize not only the VRT provided by Bugcrowd, but also the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA. CISA's KEV catalog is a curated list that details vulnerabilities known to be exploited by cyber threat actors. As KEVs are identified, they will be flagged by CISA, ensuring agency remediation efforts are prioritized for the most urgent - and potentially damaging - vulnerabilities.

WHAT IS THE CONCEPT OF OPERATION FOR THE VDP PLATFORM?

Public researchers submit reports to the VDP Platform on vulnerabilities found within federal systems of participating agencies. Upon receipt of the vulnerability reports, the vendor team screens and triages the submissions, validating reports that appear to be legitimate. The vendor communicates directly with the researcher through the first stage (i.e., the triage/initial acceptance phase). However, agencies are also able to communicate with researchers if needed.

The agency receives the report from the triage team and validates each submission. Once a submission is validated by an agency, it is the responsibility of the agency to action the vulnerability report.

Agency users have access to the VDP Platform by logging into the web-based platform interface. Agencies can view a dashboard with data specific to their program (including vulnerability submission trends and general statistics).

WHAT ARE THE BENEFITS OF HOSTING A VDP ON THE VDP PLATFORM?

Participating agencies can be listed publicly on the VDP Platform or may choose to use an embedded form on their own website. Hosting only on an agency's website limits the traffic of researchers to an agency VDP. The VDP Platform publicizes each participating agency's VDP, significantly increasing researcher attention and submissions.

IF AN AGENCY DECIDES TO OFFBOARD, WILL THEY HAVE ACCESS TO THEIR VULNERABILITY REPORTS?

Yes, the offboarded agency would be able to retrieve their data from the VDP Platform.

WHO ARE THE RESEARCHERS? WHY DO THEY PARTICIPATE?

The researcher community ranges from security and industry professionals to novices who are working to develop their skills and strengthen the cybersecurity postures of participating entities. Any person may create a researcher account and must adhere to the VDP Platform's "Code of Conduct" and responsible disclosure guidelines.

Researchers may be motivated to participate by several factors, including a sense of civic duty and skill development. Additionally, effective researchers with a record of strong performance on the VDP Platform become eligible to participate in bug bounty programs. Bug bounty programs are designed to reward researchers with financial compensation for the vulnerabilities they report.

HOW DO I SIGN UP FOR THE VDP PLATFORM?

Any agency interested in participating or receiving additional information should contact CyberSharedServices@cisa.dhs.gov.