VULNERABILITY DISCLOSURE POLICY PLATFORM

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 and collaborate with the public to improve the security of the agency's internet-accessible systems. In furtherance of CISA's issuance of Binding Operational Directive (BOD) 20-01, CISA's 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 encourages vulnerability correspondence between the public and participating agencies, providing several benefits for participating agencies such as:

- **Minimal Cost**: CISA is utilizing a shared service approach to deliver the VDP Platform, centralizing the administrative costs. CISA will cover all costs directly associated with the VDP Platform through the current lifecycle of the contract and will re-evaluate and communicate updates in Fiscal Year (FY) 2023.
- **Binding Operational Directive 20-01 Reporting:** The VDP Platform automatically facilitates the compliance reporting metrics to CISA on behalf of agencies and reduces agency reporting efforts.
- **Compliance with Federal Requirements:** CISA's Cybersecurity Quality Services Management Office (Cyber QSMO) centrally manages the VDP Platform and thus ensures the service meets all relevant government-wide standards, policies, and requirements.
- **Reduced Agency Burden:** The VDP Platform Service Provider hosts and manages the platform by overseeing administrative responsibilities, user management, and platform support. The service includes basic assessment of submitted vulnerability reports, enabling agencies to focus on reports that have a real impact.
- **Improved Information Sharing Across Federal Enterprise:** By allowing CISA to maintain insight into disclosure activities, the VDP Platform enhances interagency vulnerability information sharing.

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: Data from the service is used to track reported vulnerabilities and link related reports by reporter, vulnerability type, or other standards.

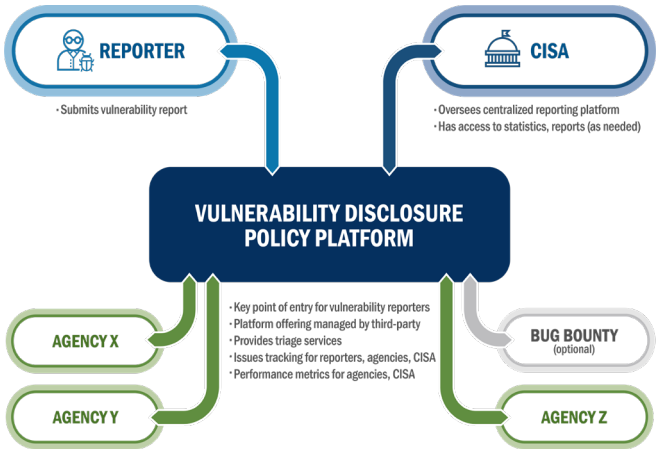
Communication: The VDP Platform provides a web-based communication mechanism between reporter and agency, and allows agency users to create and manage role-based accounts for their organization.

Application Programming Interface (API): The VDP 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.

Reporting: The service delivers reporting metrics and requirements mandated by BOD 20-01.

HOW IT WORKS

The VDP Platform is a software-as-a-service application that serves as a primary point of entry for reporters to alert participating agencies to issues on their internet accessible systems. The remediation of identified vulnerabilities on federal information systems will remain the responsibility of the agencies operating the impacted systems, not CISA or the VDP Platform Service Provider.



Individuals from the public submit reports on vulnerabilities found within federal systems of participating agencies to the centralized VDP Platform. Once they receive the reports, the VDP Platform Service Provider screens and triages the submissions, validating reports that appear to be legitimate. CISA has read-only access to all agency reports to view aggregated statistical data, and thus maintains insight into the disclosed activities but does not actively participate in each remediation process. Agency users have access to the Platform by logging into the VDP Platform interface, viewing the agency dashboard which will list vulnerability submissions and general statistics.

HOW CAN YOU REQUEST SERVICES?

Any agency interested in participating or receiving additional information should contact the Cyber QSMO at QSMO@cisa.dhs.gov.

The agency onboarding process to the VDP Platform includes:

1. Agency emails QSMO@cisa.dhs.gov and identifies the initial agency point-of-contacts to act as superusers, and the agency system(s) in scope of the VDP Platform.
2. CISA works with the VDP Platform Service Provider to establish each agency's webpage.
3. The VDP Platform prompts the agency-identified point-of-contacts (POCs) to create superuser accounts and provide supporting training documents.
4. The agency POCs log-in to the VDP Platform and customize the webpage to the agency's preference.

ABOUT THE CYBER QSMO

CISA's Cyber Quality Service Management Office (Cyber QSMO) serves as an online government storefront for high-quality cybersecurity services, aligning with federal requirements and priorities. Our mission is to centralize, standardize, automate, and offer high-quality, cost-effective cybersecurity services and products for all federal civilian departments and agencies. 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 top priorities are to understand our customers' cybersecurity needs, gaps, and risks, and to offer and continually refine service offerings that both meet those demands and align with the ever-changing threat landscape impacting the federal .gov enterprise.

OUR CYBERSECURITY MARKETPLACE

CISA's Cyber QSMO 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 Cyber 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. Our long-term vision is to advance the availability of innovative solutions for federal agencies and improve mission support functions.