VULNERABILITY DISCLOSURE POLICY (VDP) PLATFORM

CISA's Vulnerability Disclosure Policy (VDP) Platform will support 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 Platform aims to promote good faith security research, ultimately resulting in improved security and coordinated disclosure across the federal civilian enterprise.

BENEFITS

CISA's Platform encourages vulnerability correspondence between the public and participating agencies, providing several benefits to those agencies, including:

- **Compliance with Federal Requirements:** The Platform will be centrally managed by CISA's Cybersecurity Quality Services Management Office (Cyber QSMO), which will ensure the Platform meets all relevant government-wide standards, policy, and business requirements.
- **Reduced Agency Burden:** The Platform service provider will host and manage the Platform, including administrative responsibilities, user management, and support. The service will include basic assessing of vulnerability reports submitted, enabling agencies to focus on those reports that have real impact.
- **Improved Information Sharing Across Federal Enterprise:** By allowing CISA to maintain insight into disclosure activities, the Platform will increase the sharing of vulnerability information across agencies.

FUNCTIONALITY HIGHLIGHTS

The Platform will provide a primary point of entry for vulnerability reporters to alert participating agencies of potential issues on federal information systems. Below outlines some of the expected functionality of the CISA Platform.

- Screens spam and performs a base level of validation of the submitted report.
- Tracks reported vulnerabilities and link reports that are related by reporter, vulnerability type, or other purpose.
- Provides a web-based communication mechanism between the reporter and the agency.
- Allows agency users to create and manage role-based accounts for their organization or suborganizations.
- Offers an application programming interface (API) to take various actions on vulnerability reports or pull metrics.
- Delivers metrics around reports, minimizing agency burden in complying with BOD 20-01's reporting requirements.
- Gives alerts to the reporter and agency users on updates, as well as to CISA based on events of interest, metrics approaching or hitting defined thresholds, etc. These alerts should be configurable in the user interface and available via API.

Additional information regarding functionality will become available as acquisition of the Platform is completed.

HOW WILL IT WORK?

The Platform is anticipated to be a software-as-a-service application that serves as a primary point of entry for reporters to alert participating agencies of issues on the agency's 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.

- **Vulnerability Reporters:** utilize this Platform as a central place to report vulnerabilities in federal systems of participating agencies.
- **Platform Service Provider:** provides screening and initial triage of submissions, validating which appear to be legitimate.
- **CISA:** maintains insight into disclosure activities but does not actively participate in each disclosure remediation process. CISA will have read-only access to all agency reports to view aggregate statistical data and reports.
- **Your Agency:** maintains a separate profile in the Platform. By logging into the Platform interface, agency users can see an agency dashboard with the list of submissions and general statistics.
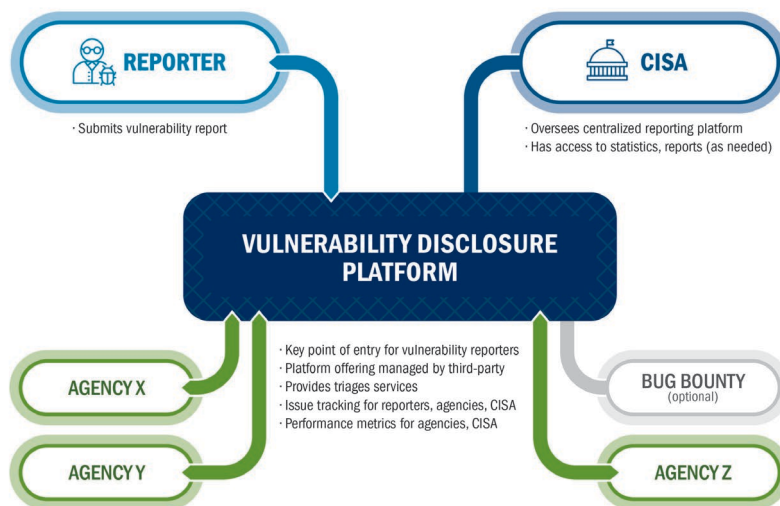
CISA's Vulnerability Disclosure Platform

HOW CAN YOU REQUEST SERVICES?

CISA anticipates that costs will be assessed for each report triaged by the service provider. CISA plans to fund a limited number of reports, on a trial basis, during the first year of performance. The Cyber QSMO will work with agencies directly to configure the Platform service in response to an agency request to participate. Any agency interested in participating or receiving additional information should contact the Cyber QSMO at QSMO@hq.dhs.gov.

CONNECT WITH US
www.cisa.gov

For more information,
email QSMO@hq.dhs.gov.

Linkedin.com/company/cybersecurity and infrastructure security agency

@CISAgov | @cyber | @uscert_gov

Facebook.com/CISA