VULNERABILTY DISCLOSURE PLATFORM

OVERVIEW

CISA's Vulnerability Disclosure Platform (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 a participating federal agency's internet-accessible systems. In furtherance of CISA's issuance of Binding Operational Directive (BOD) 20-01, CISA's Platform aims to support good faith security research, ultimately resulting in improved security and coordinated disclosure across the federal civilian enterprise. The Platform is anticipated to be available to agencies in Spring 2021.

BENEFITS

CISA's Platform encourages vulnerability correspondence between the public and participating agencies and facilitates day-to day operations associated with agencies' vulnerability disclosure policies (VDP). This provides 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 ensures 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 assessment of vulnerability reports submitted, enabling agencies to focus on high-impact reports.
- 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.

TRIAL

CISA recognizes allocating resources towards utilizing the Platform requires planning. In order to support agencies in operationalizing their VDP, CISA is offering a trial program for its Platform. The trial will cover the fixed costs associated with the Platform, as well as a specific number of reports in the first year. The number of reports that CISA will be able to fund is still being defined, as the acquisition is ongoing. However, CISA is hopeful to minimize or eliminate costs placed on agencies in the first year, and potentially beyond, pending future funding. As the trial is solidified, CISA will proactively inform agencies of updates.

FUNCTIONALITY HIGHLIGHTS

The Platform will intake, triage, and help communicate the vulnerabilities disclosed by the public to the proper agency. Below outlines some of the expected functionality of the CISA Platform.

- Screens inaccurate or repetitive reports and performs a base level validation of the submitted report.
- Tracks reported vulnerabilities and links 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, allowing agencies to pull the reports into their ticketing systems.

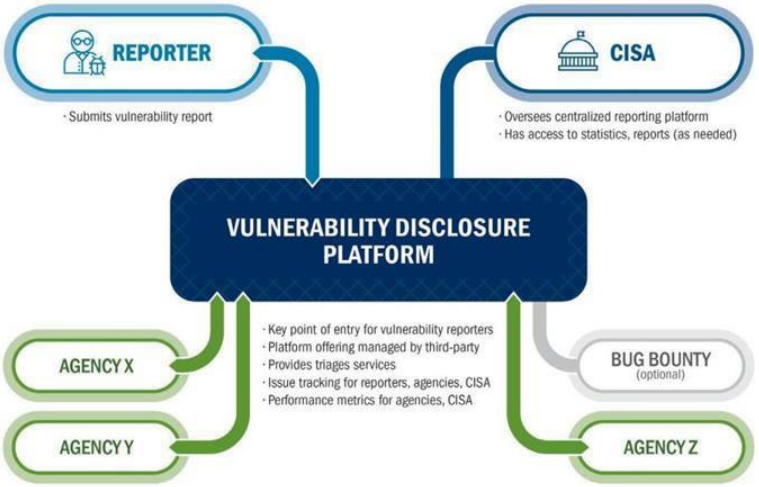
Additional information regarding functionality will become available as acquisition of the Platform is finalized.

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 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. The Platform may also be configured to integrate and support an agency's separately-authorized bug bounty program.

CISA's Vulnerability Disclosure Platform



ABOUT THE CYBER QSMO & THE CYBERSECURITY MARKETPLACE

CISA's Cyber QSMO program serves as the 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.

CISA's Cyber QSMO's Marketplace offers rigorously-vetted, 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. The Marketplace will be a dynamic customer-centric application geared at making it easier for customers to understand available cybersecurity services, access information about providers, and begin the purchasing process. The Cyber QSMO Marketplace will eventually include service offerings from commercial providers, in addition to any services offered by federal providers.

HOW CAN YOU REQUEST SERVICES?

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 OSMO@cisa.dhs.gov.