

CYBER QUALITY SERVICES MANAGEMENT OFFICE (QSMO)

SHARED SERVICES FORUM

JIM SHEIRE, QSMO BRANCH CHIEF

JUNE 10, 2021



Vulnerability Disclosure Policy Platform

In response to Binding Operational Directive (BOD) 20-01, CISA is standing up the Vulnerability Disclosure Policy (VDP) Platform to intake, triage, and communicate vulnerabilities disclosed by the public. The Cyber QSMO will centrally manage the VDP Platform to ensure it meets all relevant government-wide standards, policies, and business requirements. Additionally, the VDP Platform will enhance vulnerability information sharing across agencies.



Functionality: The VDP Platform will intake, triage, and help communicate vulnerabilities disclosed by the public to the proper agency. This service will:

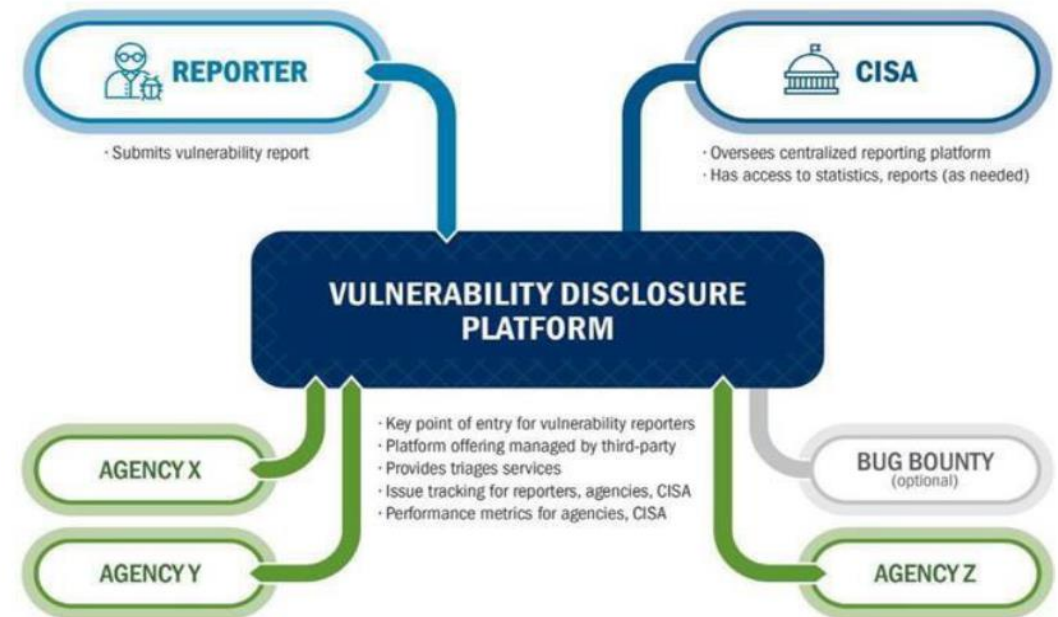
- Screen and validate reports
- Track, group, and categorize reported vulnerabilities
- Allow agencies to create and manage role-based accounts for their organization or suborganizations
- Offer an application programming interface (API) to take various actions on vulnerability reports and pull metrics



Benefits: CISA's VDP Platform aims to promote good faith security research and **improve security and coordinated disclosure** across the federal civilian enterprise. Benefits include:

- Minimal cost
- Increased information sharing across the federal enterprise
- Reduced agency burden in managing vulnerability reporting
- Compliance with federal requirements, including CISA's Binding Operational Directive (BOD) 20-01


CISA's Vulnerability Disclosure Platform




Looking Forward: VDP is executing Authority-to-Operate (ATO) processes, while expecting to deploy the service to an initial set of participating agencies in Q4 FY21.

Security Operations Services

CISA has partnered with the U.S. Department of Justice (DOJ) to offer a full spectrum of Security Operations services. Through DOJ's Justice Information Technology (IT) Service Offerings, the Cyber QSMO Marketplace offers a full range of comprehensive cybersecurity services that shield enterprises against threats while strengthening their cyber defense.

-  **Functionality:** This suite of services delivers intelligence-led, expert-driven, 24x7 threat detection, hunting, and incident response services to customers. Service areas include, but are not limited to:
- Network and System Monitoring
 - Incident Response
 - Threat Hunting
 - Forensics
 - Cyber Threat Intelligence
 - Onboarding / Customer Support

-  **Benefits:** Security Operations services provide benefits to agencies across the Federal Civilian Executive Branch (FCEB), including:
- Improved enterprise-wide visibility into cyber vulnerabilities
 - Enhanced information sharing
 - Protection of Unclassified through Top Secret information
 - Access to large-scale security operations services for smaller agencies
 - Rapid service integration and reduced onboarding time

-  **Looking Forward:** The DOJ's Security Operations services are now available [here](#) on the [Cyber QSMO Marketplace](#), together with 23 additional DOJ cyber services that are currently undergoing CISA QSMO validation.



Protective Domain Name System Resolver

CISA's Protective Domain Name System (DNS) Resolver service offering secures and blocks government web traffic from reaching malicious destinations, and alerts security organizations within agencies when incidents occur. This service uses state-of-the-art DNS technologies and commercial threat intelligence to prevent malicious DNS content from compromising government networks, devices, and information.



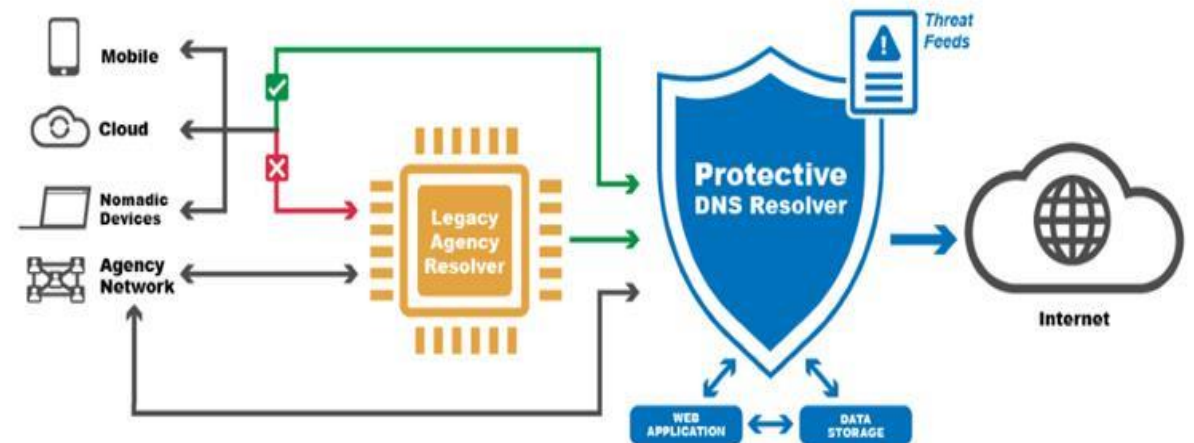
Functionality: This service offers a broad range of functionality, including:

- Real-time alerts
- Increased visibility and accessibility
- Web-app based threat reports
- Enhanced threat intelligence through multiple sources
- Alignment with zero-trust architecture



Benefits: CISA's Protective DNS service **enhances incident detection and response capabilities** and creates an enterprise network that is **more resilient to cyber attacks**, helping to better protect federal networks and information. Key benefits include:

- Seamless integration with existing agency protections
- Increased visibility and accessibility to the DNS threat landscape
- More comprehensive device coverage
- Scalability
- Compliance with legal requirements



Looking Forward: CISA awarded the Protective DNS Resolver Service through GSA's Alliant 2 Government-wide Acquisition Contract (GWAC) on April 30th.

The Cyber QSMO plans to offer CISA's Protective DNS service to the FCEB in Q2 FY22 and is currently engaging agencies to enroll and participate in our working groups and initial service deployment.

QUESTIONS AND ANSWERS





Questions?

Email: QSMO@cisa.dhs.gov
[Cyber QSMO | CISA](#)

James Sheire, Cyber QSMO Branch Chief
James.Sheire@cisa.dhs.gov

Rachel Kelly, Cyber QSMO Deputy Branch Chief
Rachel.Kelly@cisa.dhs.gov

C