Cyber QSMO – Shared Services Leadership Coalition Briefing

Agenda

1. Marketplace Overview
2. Marketplace Update
3. Designated Service Update
   ▪ Security Operations Services
   ▪ Vulnerability Disclosure Platform
   ▪ Protective DNS Resolver Service
Executive Summary

- CISA’s Cyber Quality Service Management Office (Cyber QSMO) seeks to operate a best-in-class online government marketplace for high-quality, cost-effective cybersecurity services to better secure federal networks and mitigate cyber risks.
- The Cyber QSMO’s objectives are to:
  - Reduce cyber vulnerabilities across the federal enterprise;
  - Standardize and automate cybersecurity support processes and data;
  - Reduce cyber mission support operations and maintenance costs; and
  - Create a positive customer experience for our federal civilian customers.

Marketplace Benefits

- The Marketplace centralizes, standardizes, and offers cybersecurity services and products for the federal civilian enterprise.
- By offering CISA-onboarded and validated cybersecurity services, the 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.
Update

- The Cyber QSMO launched its initial marketplace in Q1FY21.
- The Cyber QSMO Marketplace includes over 70 cybersecurity services from federal providers including:
  - U.S. Department of Transportation (DOT)
  - U.S. Department of Health and Human Services (HHS)
  - U.S. Department of Justice (DOJ)
  - Cybersecurity and Infrastructure Security Agency (CISA)

Looking Forward

- Plans are underway to offer additional CISA cybersecurity services, as well as services from other federal providers including the General Services Administration (GSA)
- The Cyber QSMO plans to offer the following OMB-designated services to the Marketplace later this fiscal year:
  - Vulnerability Disclosure Platform
  - Protective Domain Name System (DNS) Resolver Service

Looking Forward

- Plans are underway to offer additional CISA cybersecurity services, as well as services from other federal providers including the General Services Administration (GSA)
- The Cyber QSMO plans to offer the following OMB-designated services to the Marketplace later this fiscal year:
  - Vulnerability Disclosure Platform
  - Protective Domain Name System (DNS) Resolver Service
Cyber QSMO – Shared Services Leadership Coalition Briefing

3. Designated Service Update: 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 24x7 threat monitoring, detection and incident response, threat intelligence, and cybersecurity investigations to customers via the Justice Security Operations Center (JSOC). Service areas include, but are not limited to:

- Vulnerability Asset Management
- Cyber Hunt
- Awareness and Training
- Security Continuous Monitoring
- Threat Intelligence
- Governance 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.
CISA’s Vulnerability Disclosure Platform (Platform) will help agencies streamline day-to-day operations when disclosing and managing cyber vulnerabilities. The Platform serves as the primary point of entry for intaking, triaging, and routing vulnerabilities disclosed by the public (i.e., ethical hackers).

**Functionality:** The 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 Platform supports good faith security research and improves security and coordinated disclosure across the federal civilian enterprise. Benefits include:
- 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

**Looking Forward:** With the protest resolved, plans are underway to obtain an ATO and deploy the service in June 2021 to an initial set of participating agencies. Over 20 customers have enrolled in the initial service deployment.
3. Designated Service Update: Protective DNS Resolver Service

CISA’s Protective DNS Resolver service employs state-of-the-art DNS technologies and commercial threat intelligence to neutralize malicious DNS content.

**Functionality:** This service offers a broad range functionality, including:
- Real-time alerts
- Web-app based threat reports
- Enhanced threat intelligence through multiple threat 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. This service also promotes:
- Seamless integration with existing agency protections
- Increased visibility and accessibility to the DNS threat landscape
- More comprehensive device coverage
- Scalability
- Compliance with legal requirements
- Protection against maladvertising

**Looking Forward:** CISA released a Request for Proposal through GSA’s Alliant 2 Government-wide Acquisition Contract (GWAC) last week, and plans to award the contract in early Q2 for CY21.

The Cyber QSMO is planning to offer CISA’s Protective DNS service to federal civilian agencies and departments. The Cyber QSMO will be engaging agencies to enroll and participate in our initial service deployment in coming months.
James Sheire, Cyber QSMO Branch Chief
James.Sheire@cisa.dhs.gov

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

Cristina Perez, Cyber QSMO Customer Experience and Communications Lead
Cristina.Perez@cisa.dhs.gov