CSD SHARED SERVICES OVERVIEW

SHARED SERVICES LEADERSHIP COALITION MONTHLY MEETING

September 2024

Agenda

- Cyber QSMO Explained
- Cyber QSMO Services
- CISA's Service Delivery Approach
- CISA's Cyber Shared Services
- Current Opportunities
- On the Horizon for CISA

Cyber QSMO Explained

CISA provides critical, enterprise-wide cybersecurity services and programs to ensure the security of federal networks.

- **Issue:** Cybersecurity maturity varies by agency. As a result, the Federal Government faces common, significant challenges in securing information technology and mitigating cybersecurity risks.
- **OMB Requirement:** In April 2020, The Office of Management and Budget (OMB) formally designated CISA as the Cybersecurity QSMO. This designation coincided with the one-year anniversary of OMB *Memorandum 19-16: Centralized Mission Support Capabilities for the Federal Government.*

Federal Government cybersecurity spending was projected at $7.8 billion in FY20, with over 2 million users on 6,500+ IT systems.

The Cyber QSMO was charged with modernizing shared services governance, development, and distribution.

Cyber QSMO Services

	Protective Domain name System (DNS) Resolver Provider – CISA	Vulnerability Disclosure Policy (VDP) Platform Provider – CISA	Security Operations Provider – DOJ
OVERVIEW OF SERVICE	✓ Unclassified-only intel feeds ✓ Device-centric, not network centric (aligns to zero trust concepts) ✓ Speed and ease for CISA analysts to update blocklists ✓ Log everything, enable enterprise security insight ✓ Secure, encrypted DNS resolution to protect data in transit	✓ Tracks reported vulnerabilities ✓ Provides web-based, bi-directional communication with the reporters ✓ Allows agency to create and manage role-based accounts. ✓ Enables the creation and analysis of vulnerability reports. ✓ Alerts relevant users when updates are made, events of interest occur, or pre-defined thresholds are met.	✓ OMB-designated Federal Shared Services Center ✓ Unclassified through Top Secret environment protection ✓ Intelligence-led, expert-driven 24x7 detection, hunting, and response ✓ Economies of scale, skills and capabilities.
OBJECTIVE	• **Helps prevent future threats** • **Protects a wider range of devices and traffic** • **Improves customers' and CISA's ability to respond to cybersecurity incidents**	• **Promote good faith security research** • **Reduces the burden of compliance with policy requirements** • **Improves security and coordinated disclosure across the federal civilian enterprise**	• **Full spectrum of cybersecurity operations services** • **Helps customers meet rapidly evolving operational needs** • **Decreases total cost of ownership and related procurement and management burdens**

CISA's Service Delivery Approach

What You See: Evolution of the Cyber QSMO into the Cybersecurity Shared Services Office (CSSO)

CISA has established a more holistic approach to delivering services that better meets agencies needs and is more responsive to the ever-evolving risk landscape. This includes:

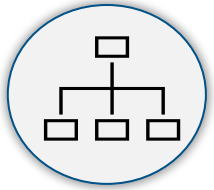
- Facilitating Federal provided services in a centralized manner to help agencies identify and leverage services peer agencies provide.
- Developing and making available shared services with commercial providers to provide agencies with cutting-edge, cost-effective cybersecurity solutions.

A Peak Behind the Scenes: CISA's Cybersecurity Division (CSD) as a Service Delivery Organization

Internally CISA's Cybersecurity Division is working to mature the way it "delivers" (and ideates, prioritizes, develops, deploys, and manages) services, by developing a Service holistic operating model.

CISA's Cybersecurity Division is taking action to standardize and improve the way it delivers its full portfolio of risk reducing services to external stakeholders. It has defined and is implementing a new Service Delivery Organization (SDO) Operating Model that will drive improvements in service onboarding, usage, performance, transparency, and reliability, while reducing redundant efforts.

CISA as a Provider



Managed Service

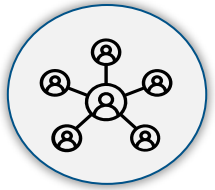
Managed services will **acquire, deliver, and manage shared services** for use by customers, reducing risk either directly via provision of protective capabilities or indirectly via informing the customer of their risk posture to enable action.

Protective DNS
Threat Intelligence Enterprise Services
Vulnerability Scanning
CDM: Identity as a Service

Integration Service

Integration services will **support organizations with the acquisition and implementation** of tools and capabilities, in many cases transitioning the ownership, management, and maintenance to the customer, supporting the establishment of base cybersecurity capabilities.

CDM: Asset Management
CDM: Network Security Management
CyberSentry



Professional Service

Professional services will **provide discrete services to stakeholders and customers to address operational needs**, informing both their posture and helping to remediate realized threats.

Red Team Assessments
Critical Product Evaluation
Cyber Incident Response
Risk and Vulnerability Assessments

The development of an Open-Source Service Delivery Model is under active analysis.

CISA as a Broker

Brokered Service

Brokered services will establish scalable partnerships with robust requirements, **enabling customers to select and onboard to services** in a streamlined manner.

CISA's broker model offers federal agencies and eligible SLTT an opportunity to acquire high-quality, cost-efficient cybersecurity services that meet or exceed government standards and requirements.

CISA has currently validated several federal shared service provider agencies and is developing an approach to improve the standards and requirements of commercial shared service providers in certain service areas on GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) contracts.

Department of Health and Human Services
Department of the Interior
Department of Justice
Department of Transportation
Multi-State Information Sharing and Analysis Center

FY24 Q4 Opportunities

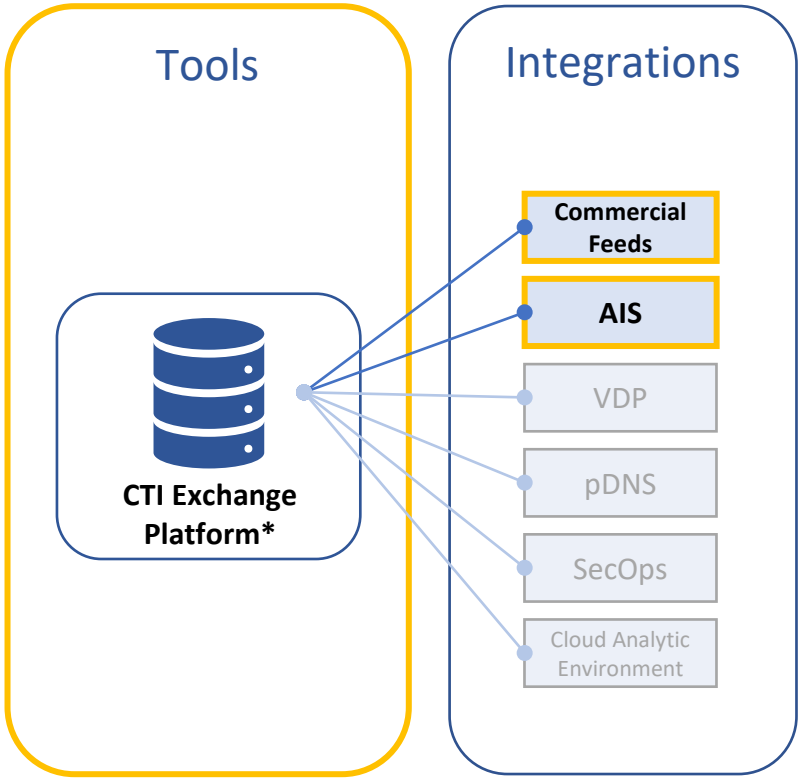
In Q4, CISA's Cybersecurity Shared Services Office will double-down on promoting its open-source software solutions.

- **Logging Made Easy:** A self-install tool on GitHub that allows users to easily administer centralized log management.
- **MALCOM:** An accessible, all-in-one intelligence toolkit that allows empowers companies with quality security insights.
- **Secure Cloud Business Applications:** A suite of guidance and cloud-based solutions for enterprise cybersecurity.

Logging Made Easy	MALCOM	SCuBA
✓ Available worldwide to small-to-medium sized organizations	✓ Available to U.S. critical infrastructure communities	✓ Available to federal agencies and some, select critical infrastructure partners
✓ Provides free, centralized log management and monitoring capabilities for enterprises running on Windows systems	✓ Delivers contextualized threat intelligence data to enhance OT/IT security on virtually all operating systems	✓ Serves as a resource library for guidance on cloud-based technical solutions
✓ Improves organizational analytics and enables custom filtering through Wingbeat event collection and Elasticsearch.	✓ Offers enhanced analysis and data visualization through OpenSearch Dashboard and Arkime	✓ Provides access to exclusive tools – SCuBA Gear and Goggles – that help users assess the health of their cloud environments

On the Horizon from CISA

Threat Intelligence Enterprise Services (TIES) – FY25



VALUE PROPOSITION

- CISA intends for TIES to serve as a one stop shop for its entire cyber threat intelligence (CTI) services portfolio. TIES will provide agencies with cutting edge tools, services, and guidance to help them generate, share, and effectively use CTI to defend their enterprise.

BENEFITS

- TIES will provide agencies with access to high-confidence, actionable CTI in a singular location that can integrate with disparate tools and capabilities.
- TIES will enable agencies to seamlessly triage, analyze, and share high-confidence CTI, empowering the entire community to defend against advanced and evolving threats.

USER COMMUNITIES

- In the beginning, TIES will be available for FCEB users only. Over time, CISA aims to extend availability to the Department of Defense, Critical Infrastructure, state, local, tribal, and territorial communities.

Questions or Feedback?

cybersharedservices@cisa.dhs.gov