CYBERSECURITY QUALITY SERVICES MANAGEMENT OFFICE (CYBER QSMO)

Overview

Cyber QSMO

A trusted advisor for cybersecurity service strategy and management

WHO WE ARE

CISA's Cyber QSMO is the single shared service office for managing cybersecurity solutions for the U.S. Government and potentially beyond.

WHAT WE DO

We centralize, standardize, and offer high-quality cybersecurity services and capabilities to our customers, and provide integration and adoption support.

THE VALUE WE PROVIDE

Our efforts to standardize and automate processes and data collection ultimately work to reduce operations and maintenance costs for customers

Using customer insights to drive value

Asking key questions and collecting customer data throughout the process, enhances CISA's ability to provide value to agencies

Service Development

Conducting methodological due diligence about customer needs saves time later:

Who are our customers?
What do they need?
Why now?

Service Implementation

Strategic communications fueled by customer insights ensure agencies receive the right support and information

Service Management

Customer experience metrics can be collected early and can be leading indicators for overall mission impact

Who is using the service the why? Is it what we expected?
What is working about the service?
What are the pain points?
What improvements would make it work better for people?

Service Evaluation

Customer insights help identify service improvements or service end of life

Current Cyber QSMO Services

Service	Capabilities Delivered	How QSMO Supports CISA Missions
Vulnerability Disclosure Platform (VDP)	○ Tracks reported vulnerabilities, links reports by reporter and vulnerability type, and delivers metrics ○ Minimizes costs for agencies and the federal government while reducing burdens associated with VDP operations while facilitating and automating BOD 20-01 Reporting	○ Enables visibility on agency disclosed vulnerabilities ○ Supports vulnerability information sharing and response activities
Protective Domain Name System (DNS) Resolver	○ Enhanced DNS resolver protects internet traffic from malicious domains while allowing support for newer, encrypted DNS protocols and wider variety of threat intelligence integration ○ Enables greater asset coverage beyond traditional network perimeters – easier integration with cloud and mobile devices ○ Web based platform delivers real-time updates, data analytics, and management of organization-specific filters	○ Increases visibility into patterns and trends, enabling enhanced protection and the facilitation of incident response activities ○ Enhances insight into how cyber threats utilize DNS to cause harm ○ Facilitates threat correlation and automated downstream defensive actions
Security Operations Services (SOC)	○ Designed to improve enterprise-wide visibility into cyber vulnerabilities, incident discovery, and information sharing within the Federal Civilian Executive Branch (FCEB), and to provide agencies with intelligence-led, expert-driven, 24x7 threat detection, hunting, and incident response services	○ Provides standards-based security operations services to FCEB ○ Enables consolidated service performance metrics based on service provider service level agreements (SLAs) and quarterly reports

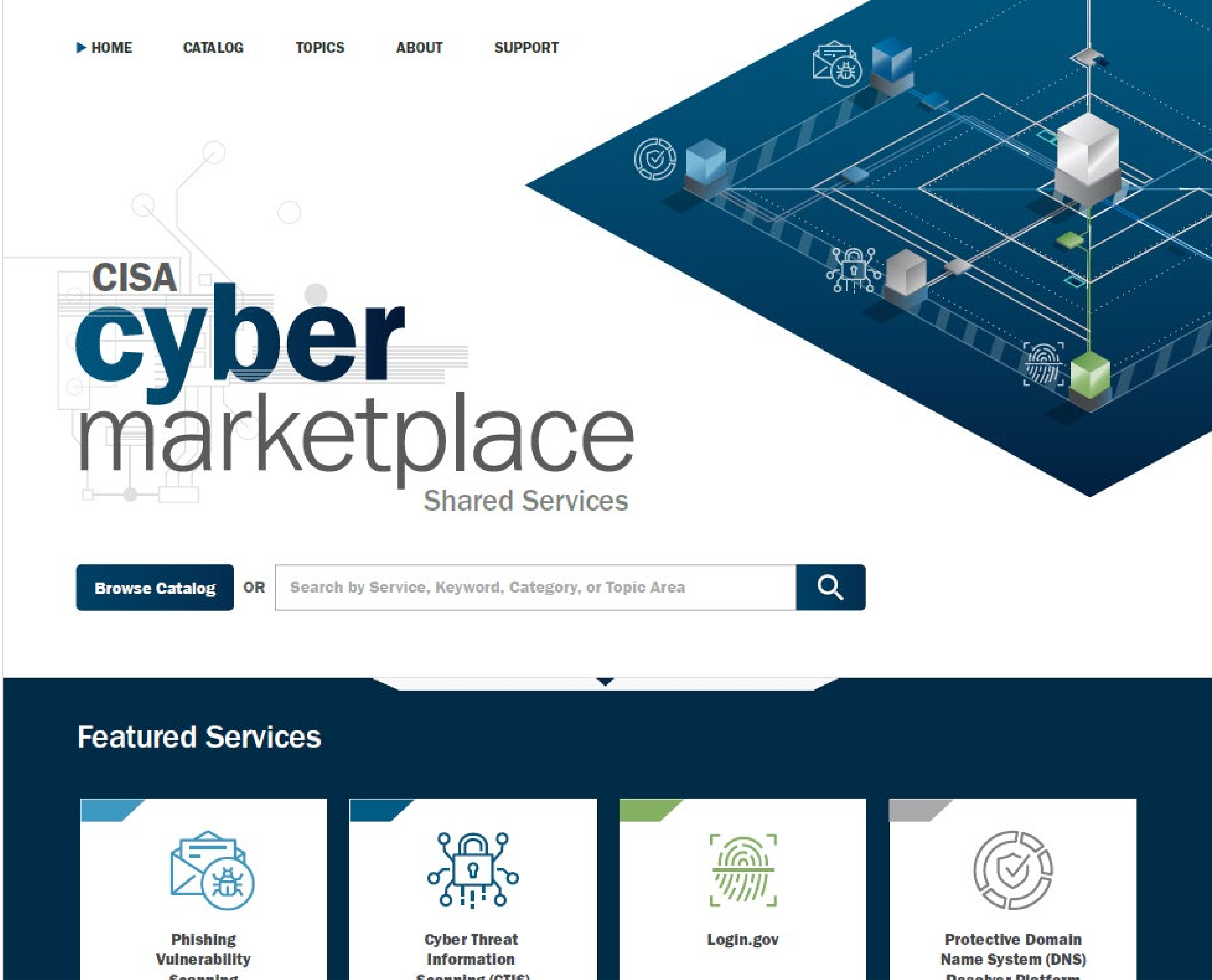
What's Next:

CISA Cybersecurity Shared Services Marketplace

Cyber Marketplace

Shopper Experience

[landing page design]



▶ HOME   CATALOG   TOPICS   ABOUT   SUPPORT

CISA cyber marketplace Shared Services

Browse Catalog OR Search by Service, Keyword, Category, or Topic Area 🔍

Featured Services

Phishing Vulnerability Scanning

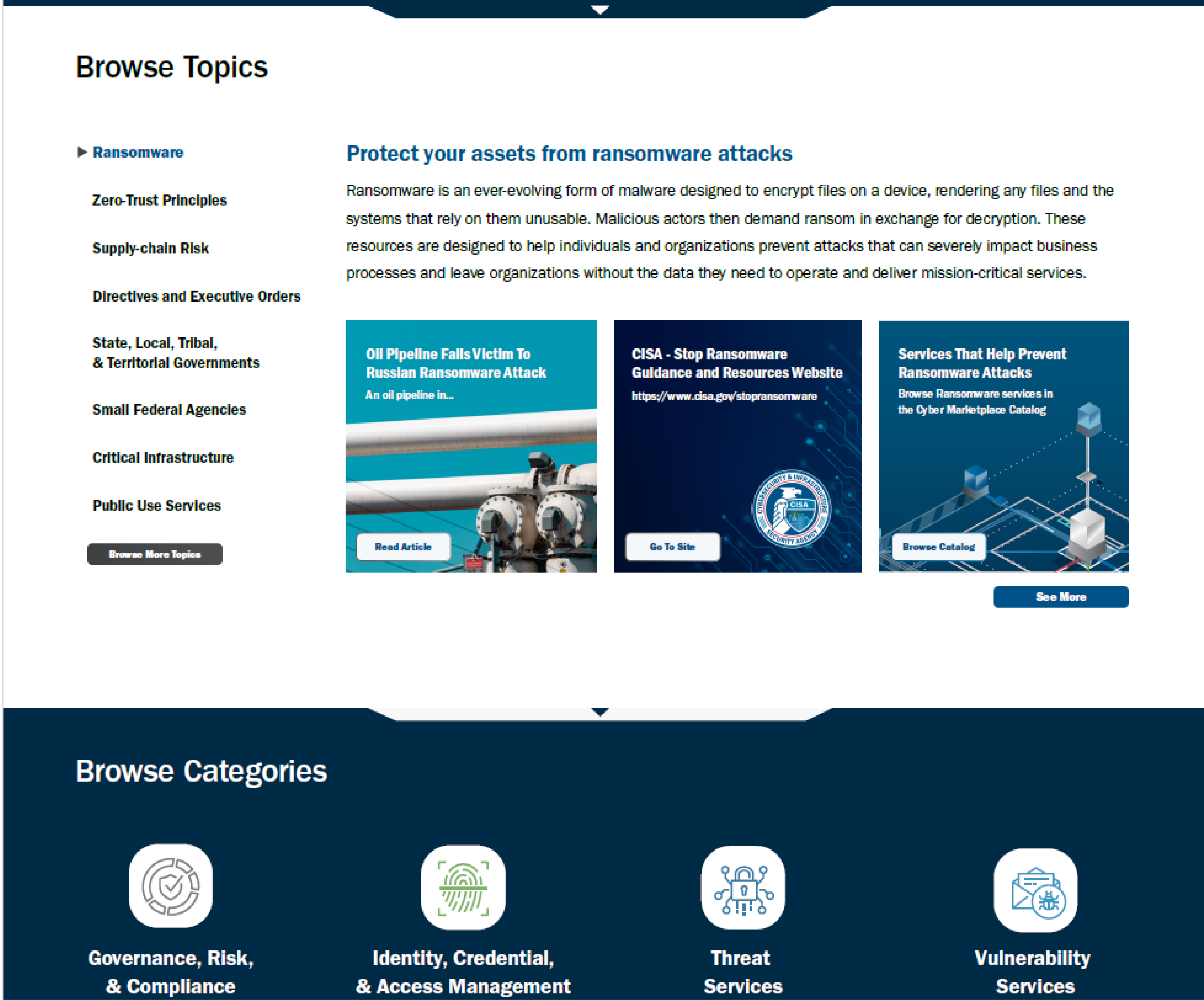
Cyber Threat Information Scanning (CTIS)

Login.gov

Protective Domain Name System (DNS) Resolver Platform

Cyber Marketplace

Shopper Experience [landing page design]



Browse Topics

- ▶ Ransomware
- Zero-Trust Principles
- Supply-chain Risk
- Directives and Executive Orders
- State, Local, Tribal, & Territorial Governments
- Small Federal Agencies
- Critical Infrastructure
- Public Use Services

Protect your assets from ransomware attacks

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Oil Pipeline Falls Victim To Russian Ransomware Attack

An oil pipeline in...

CISA - Stop Ransomware Guidance and Resources Website

https://www.cisa.gov/stopransomware

Services That Help Prevent Ransomware Attacks

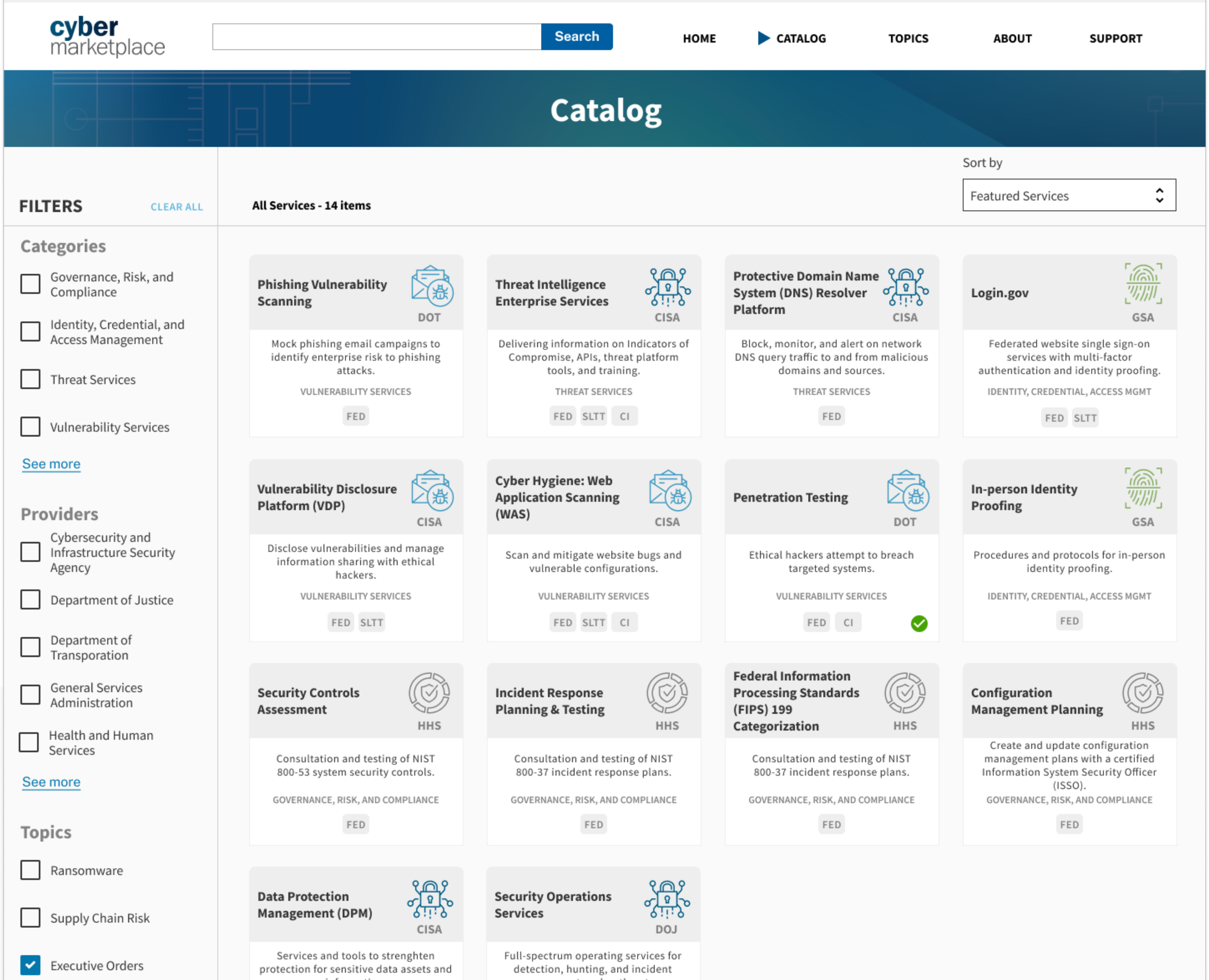
Browse Ransomware services in the Cyber Marketplace Catalog

Browse Categories

- Governance, Risk, & Compliance
- Identity, Credential, & Access Management
- Threat Services
- Vulnerability Services

Cyber Marketplace

Shopper Experience [catalog design]



Catalog

Sort by

Featured Services

FILTERS CLEAR ALL

All Services - 14 items

Categories

□ Governance, Risk, and Compliance

□ Identity, Credential, and Access Management

□ Threat Services

□ Vulnerability Services

See more

Providers

□ Cybersecurity and Infrastructure Security Agency

□ Department of Justice

□ Department of Transportation

□ General Services Administration

□ Health and Human Services

See more

Topics

□ Ransomware

□ Supply Chain Risk

☑ Executive Orders

Phishing Vulnerability Scanning DOT

Mock phishing email campaigns to identify enterprise risk to phishing attacks.

VULNERABILITY SERVICES

FED

Threat Intelligence Enterprise Services CISA

Delivering information on Indicators of Compromise, APIs, threat platform tools, and training.

THREAT SERVICES

FED SLTT CI

Protective Domain Name System (DNS) Resolver Platform CISA

Block, monitor, and alert on network DNS query traffic to and from malicious domains and sources.

THREAT SERVICES

FED

Login.gov GSA

Federated website single sign-on services with multi-factor authentication and identity proofing.

IDENTITY, CREDENTIAL, ACCESS MGMT

FED SLTT

Vulnerability Disclosure Platform (VDP) CISA

Disclose vulnerabilities and manage information sharing with ethical hackers.

VULNERABILITY SERVICES

FED SLTT

Cyber Hygiene: Web Application Scanning (WAS) CISA

Scan and mitigate website bugs and vulnerable configurations.

VULNERABILITY SERVICES

FED SLTT CI

Penetration Testing DOT

Ethical hackers attempt to breach targeted systems.

VULNERABILITY SERVICES

FED CI ✓

In-person Identity Proofing GSA

Procedures and protocols for in-person identity proofing.

IDENTITY, CREDENTIAL, ACCESS MGMT

FED

Security Controls Assessment HHS

Consultation and testing of NIST 800-53 system security controls.

GOVERNANCE, RISK, AND COMPLIANCE

FED

Incident Response Planning & Testing HHS

Consultation and testing of NIST 800-37 incident response plans.

GOVERNANCE, RISK, AND COMPLIANCE

FED

Federal Information Processing Standards (FIPS) 199 Categorization HHS

Consultation and testing of NIST 800-37 incident response plans.

GOVERNANCE, RISK, AND COMPLIANCE

FED

Configuration Management Planning HHS

Create and update configuration management plans with a certified Information System Security Officer (ISSO).

GOVERNANCE, RISK, AND COMPLIANCE

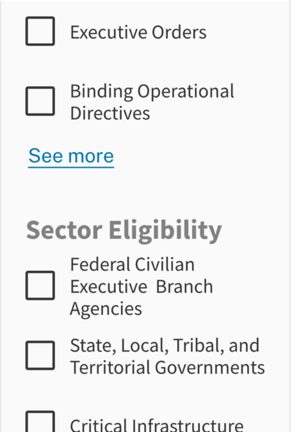
FED

Data Protection Management (DPM) CISA

Services and tools to strenghten protection for sensitive data assets and

Security Operations Services DOJ

Full-spectrum operating services for detection, hunting, and incident



□ Executive Orders

□ Binding Operational Directives

See more

Sector Eligibility

□ Federal Civilian Executive Branch Agencies

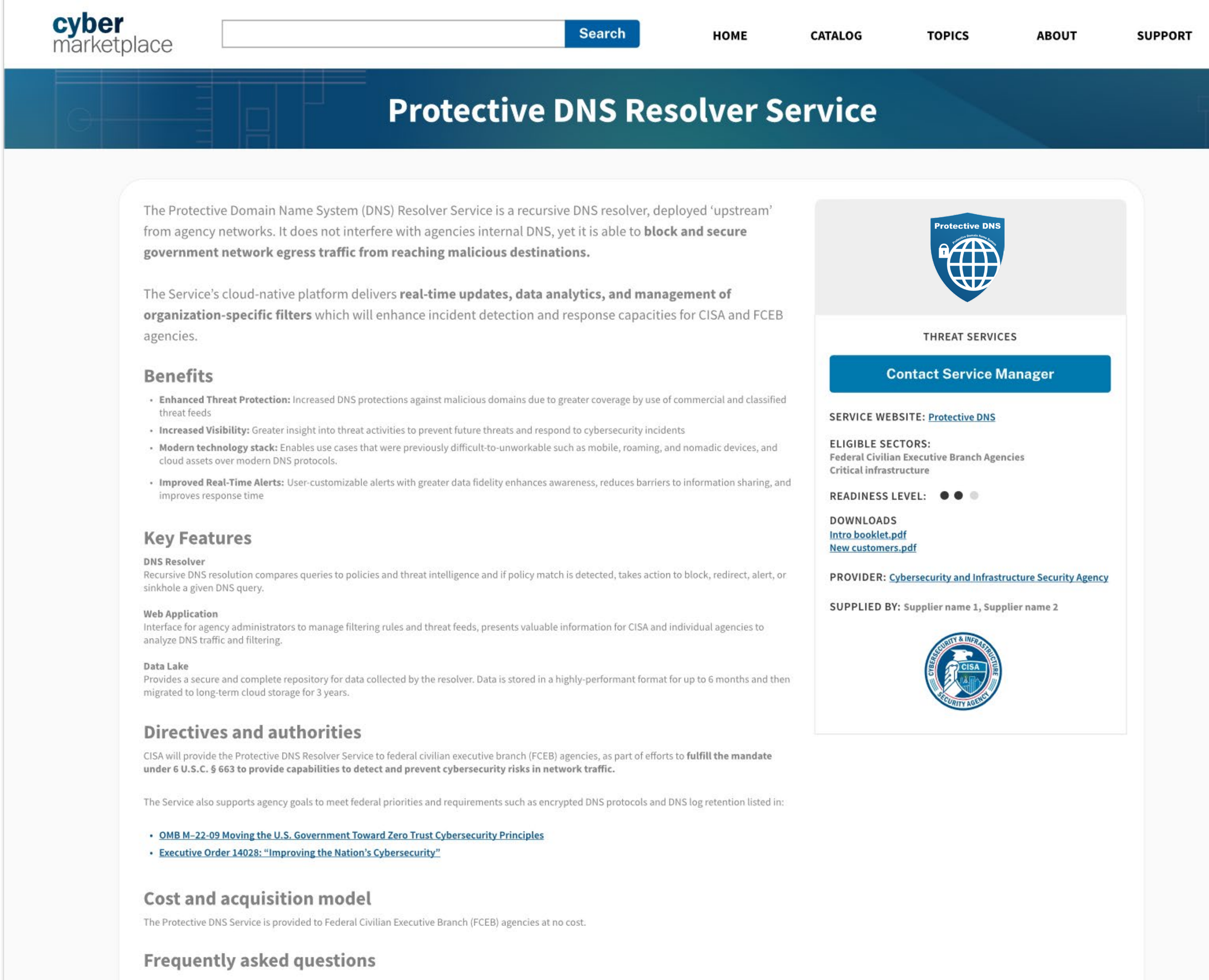
□ State, Local, Tribal, and Territorial Governments

□ Critical Infrastructure

Cyber Marketplace

Shopper Experience

[service page design]



Protective DNS Resolver Service

The Protective Domain Name System (DNS) Resolver Service is a recursive DNS resolver, deployed ‘upstream’ from agency networks. It does not interfere with agencies internal DNS, yet it is able to **block and secure government network egress traffic from reaching malicious destinations.**

The Service’s cloud-native platform delivers **real-time updates, data analytics, and management of organization-specific filters** which will enhance incident detection and response capacities for CISA and FCEB agencies.

Benefits

- **Enhanced Threat Protection:** Increased DNS protections against malicious domains due to greater coverage by use of commercial and classified threat feeds
- **Increased Visibility:** Greater insight into threat activities to prevent future threats and respond to cybersecurity incidents
- **Modern technology stack:** Enables use cases that were previously difficult-to-unworkable such as mobile, roaming, and nomadic devices, and cloud assets over modern DNS protocols.
- **Improved Real-Time Alerts:** User-customizable alerts with greater data fidelity enhances awareness, reduces barriers to information sharing, and improves response time

Key Features

DNS Resolver
Recursive DNS resolution compares queries to policies and threat intelligence and if policy match is detected, takes action to block, redirect, alert, or sinkhole a given DNS query.

Web Application
Interface for agency administrators to manage filtering rules and threat feeds, presents valuable information for CISA and individual agencies to analyze DNS traffic and filtering.

Data Lake
Provides a secure and complete repository for data collected by the resolver. Data is stored in a highly-performant format for up to 6 months and then migrated to long-term cloud storage for 3 years.

Directives and authorities

CISA will provide the Protective DNS Resolver Service to federal civilian executive branch (FCEB) agencies, as part of efforts to **fulfill the mandate under 6 U.S.C. § 663 to provide capabilities to detect and prevent cybersecurity risks in network traffic.**

The Service also supports agency goals to meet federal priorities and requirements such as encrypted DNS protocols and DNS log retention listed in:

- OMB M–22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- Executive Order 14028: “Improving the Nation’s Cybersecurity”

Cost and acquisition model

The Protective DNS Service is provided to Federal Civilian Executive Branch (FCEB) agencies at no cost.

Frequently asked questions

THREAT SERVICES

Contact Service Manager

SERVICE WEBSITE: Protective DNS

ELIGIBLE SECTORS:
Federal Civilian Executive Branch Agencies
Critical infrastructure

READINESS LEVEL: ● ● ○

DOWNLOADS
Intro booklet.pdf
New customers.pdf

PROVIDER: Cybersecurity and Infrastructure Security Agency

SUPPLIED BY: Supplier name 1, Supplier name 2

More information:

CISA Website

https://www.cisa.gov/

Cyber QSMO Website

https://www.cisa.gov/cyber-qsmo

Contact us:

QSMO@cisa.dhs.gov