
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
FEDERAL NETWORKS CONFERENCE
2024

Agenda

- Key CISA Efforts to Help Agencies Address Network Security Challenges
- What CISA Would Like to See From Industry
- What to Expect for Upcoming CDM Program Opportunities

3 FOCAL Plan: What and Why?

PRIORITY AREAS:

- **Asset Management**
- **Vulnerability Management**
- **Defensible Architecture**
- **Cyber Supply Chain Risk Management**
- **Incident Detection and Response**

WHAT IS THE FOCAL PLAN?

This plan captures the essential components of ***operational cybersecurity*** at both the agency and enterprise levels and focuses attention on capability gaps, seeking to align the elements needed to enhance our collective cyber defenses; optimizing our coordination and information sharing mechanisms; and enabling effective and interactive cybersecurity operations.

WHY IS IT IMPORTANT?

The FOCAL Plan is a shift from each federal agency managing cybersecurity individually to all of us managing our cybersecurity collectively - **as ONE federal enterprise.** It guides our collective efforts to deter, detect, and respond to cyber threat actors.

4 FOCAL Plan: Alignment Goals & Focal Points

PRIORITY AREAS	ALIGNMENT GOALS	FOCAL POINTS
Asset Management	• Increase Operational Visibility	
Vulnerability Management	• Manage the Attack Surface of Internet-Accessible Assets	Enroll in CISA's Federal Attack Surface Testing (FAST) service. Prioritize resources and document specific steps for remediating FAST findings.
Defensible Architecture	• Secure Cloud Business Applications • Share Cloud Telemetry Data with CISA • Establish Zero Trust Culture Across the Federal Enterprise	Implement the SCuBA Minimum Viable Secure Configuration Baseline by using either the ScubaGear (M365) or ScubaGoggles (GWS) assessment tools.
Cyber Supply Chain Risk Management (C-SCRM)	• Prepare for FASCSA Removal and/or Exclusion Orders • Advance Agency Enterprise C-SCRM Programs	Provide CISA with persistent access to EDR solutions to enable proactive threat hunting activities and a coordinated response to advanced threats.
Incident Detection and Response	• Enable CISA's Persistent Access Capability (PAC) • Advance SOC Governance	Validate SOC visibility into HVAs and internet-facing systems to ensure the reported M-21-31 event logging (EL) tier data is available to the SOC.

5 CISA's Zero Trust Initiative

STRONG IN CONTENT AND COMMUNITY

CISA is focused on developing **guidance and resources** that address known gaps and timely needs as agencies implement ZTA principles and in **bringing implementers together** to share approaches and lessons with each other.

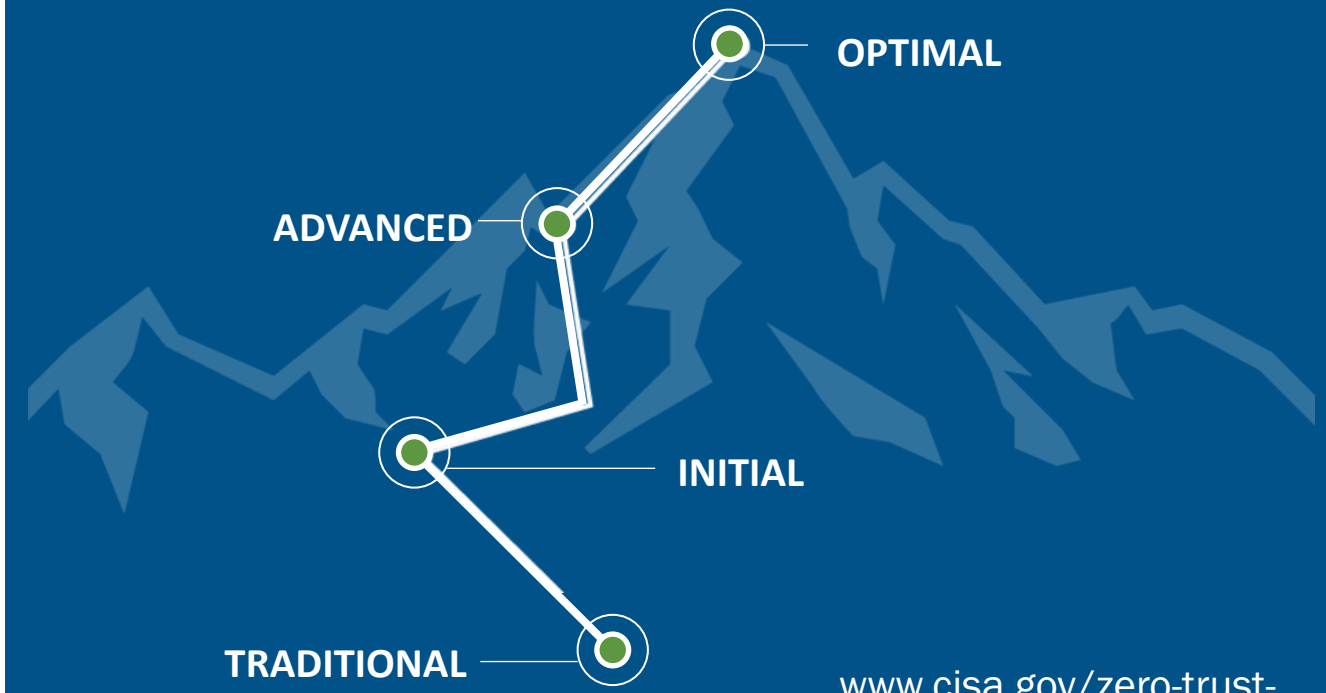
PRACTICAL GUIDANCE

TRAINING

MATURITY ASSESSMENT

Zero Trust Maturity Model 2.0

Provides an approach to help organizations along their journey to zero trust, factoring in existing investments and progress.



www.cisa.gov/zero-trust-maturity-model

6 Secure by Design

"Every technology provider must take ownership at the executive level to ensure their products are secure by design."

CISA'S SbD PLEDGE

A voluntary pledge for software manufacturers to make a good-faith effort to work towards seven goals within a year of signing:

1. Increase the use of multi-factor authentication
2. Reduce default passwords
3. Reduce prevalence of one or more vulnerability class
4. Increase the installation of security patches by customers
5. Publish a Vulnerability Disclosure Policy (VDP)
6. Demonstrate transparency in vulnerability reporting
7. Increase in the ability for customers to gather evidence of cybersecurity intrusions

HOW TO SIGN:

https://www.cisa.gov/securebydesign/pledge

7 Modernizing FedRAMP

Orienting Around the Customer Experience

01

Cybersecurity Leadership

02

Scaling a Trusted Marketplace

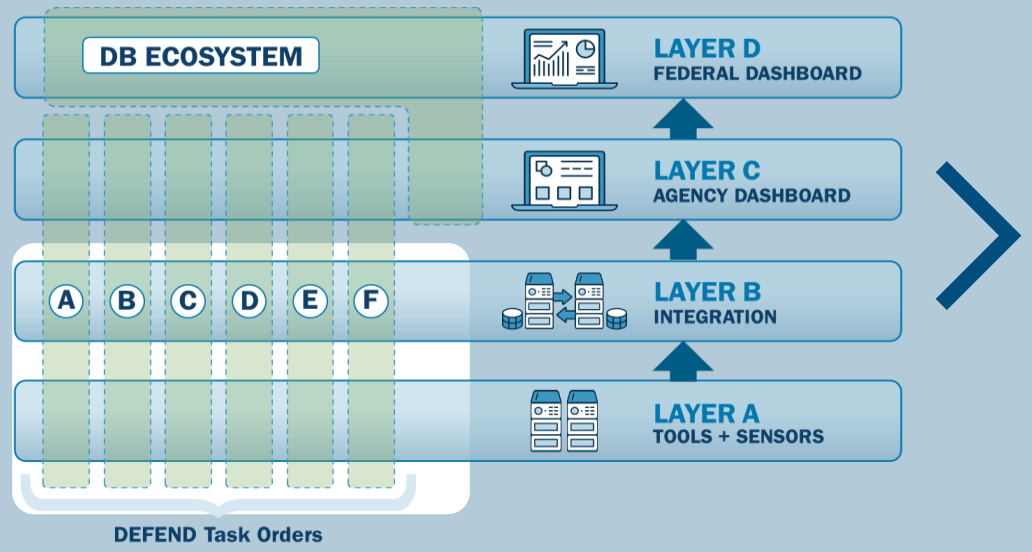
03

Smarter, Technology-Forward Operations

04

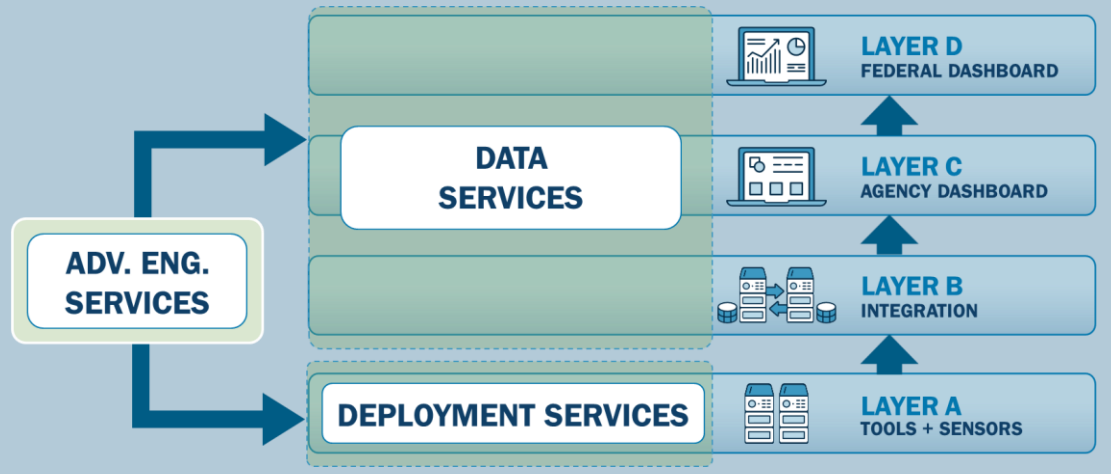
8 The Evolution of CDM Acquisition

Existing Contracting Structure on DEFEND



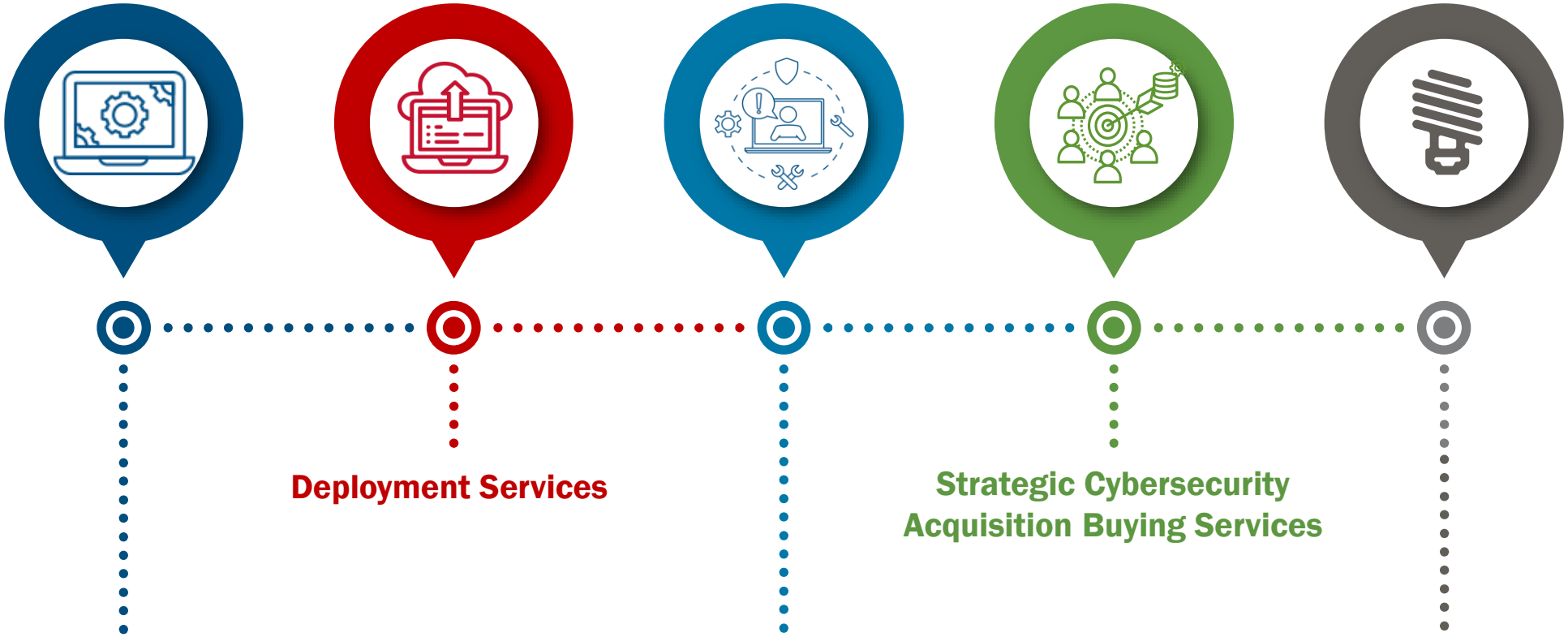
Multiple, parallel DEFEND orders led to disparate solutions, each with **unique characteristics.**

NextGen Contracting Structure



Reallocate the existing DEFEND scope into a **functionally aligned set of orders.**

9 Upcoming Opportunities



Advanced Engineering Services

Deployment Services

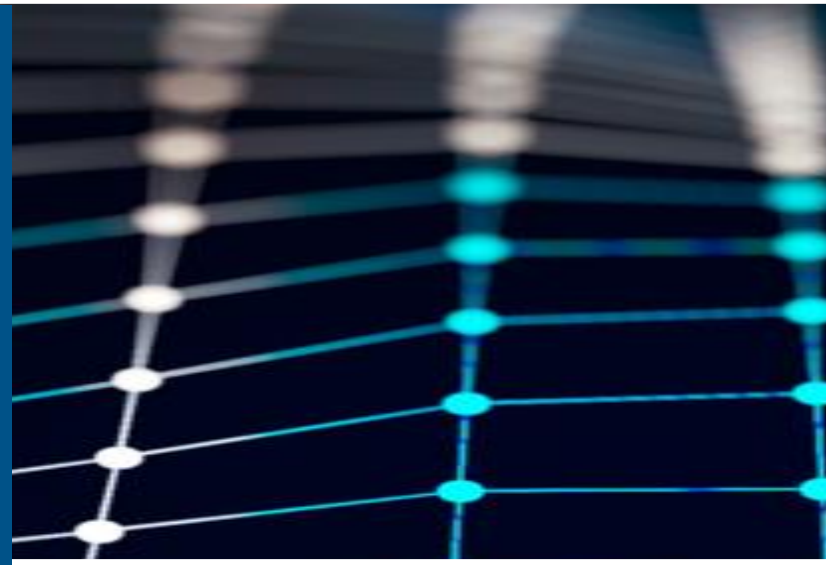
Functionally aligned to operations

Strategic Cybersecurity Acquisition Buying Services

Technical and Engineering Subject Matter Expertise Support Services

10 Doing Business With Us

- **GENERAL INQUIRIES:** CISAIndustryEngagement@cisa.dhs.gov.
- **SMALL BUSINESS OPPORTUNITIES:** The Acquisition Planning Forecast System (https://apfs-cloud.dhs.gov/) can help identify procurement opportunities early in the acquisition process.
  - **APFS INQUIRIES:** apfs-inquiries@cisa.dhs.gov.
- **CYBERSECURITY CAPACITY BUILDING MISSION:** https://www.cisa.gov/about/doing-business-cisa/doing-business-capacity-building



Q&A