DON / DoD Zero Trust Metrics Collection System

Controlled by: Department of the Navy | Controlled by: DON CIO | CUI Category: | Distribution A: For Public Release; Unlimited Distribution | POC: Kateryna Alkorn, PhD

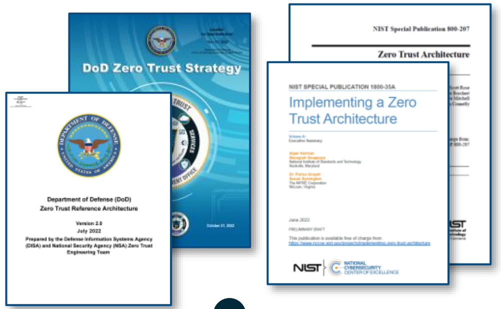
“Zero trust (ZT) is the term for an evolving set of **cybersecurity** paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources” - Zero Trust Architecture, NIST SP 800-207

Slide adapted from a presentation by Mr. David Voelker, DON CIO Zero Trust Lead

A Brief History of ZT within DoD and DON

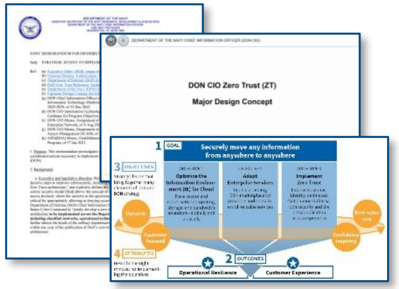
2021

President issued **Executive Order (EO) 14028, Improving the Nation's Cybersecurity,** initiating the Federal Government's migration to a zero trust architecture (ZTA).


DoD Zero Trust Strategy
Department of Defense (DoD) Zero Trust Reference Architecture
NIST Special Publication 800-207
Zero Trust Architecture
NIST SPECIAL PUBLICATION 1800-35A
Implementing a Zero Trust Architecture

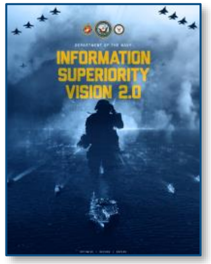
2022

DoD releases ***Zero Trust Reference Architecture*** and ***Zero Trust Strategy;*** NIST releases ***SP 800-207 Zero Trust Architecture*** and ***SP 1800-35A Implementing a Zero Trust Strategy***



2023

DON releases ***Strategic Intent for Zero Trust***, ***Capstone Design Concept for Information Superiority, Major Design Concepts for Zero Trust***, ***Navy Zero Trust Implementation Plan***



2024

DON CIO releases ***Information Superiority Vision 2.0*** highlights ZT as number 1 priority for making DON networks defendable and survivable by design

DON ZT I-Plan 2.0

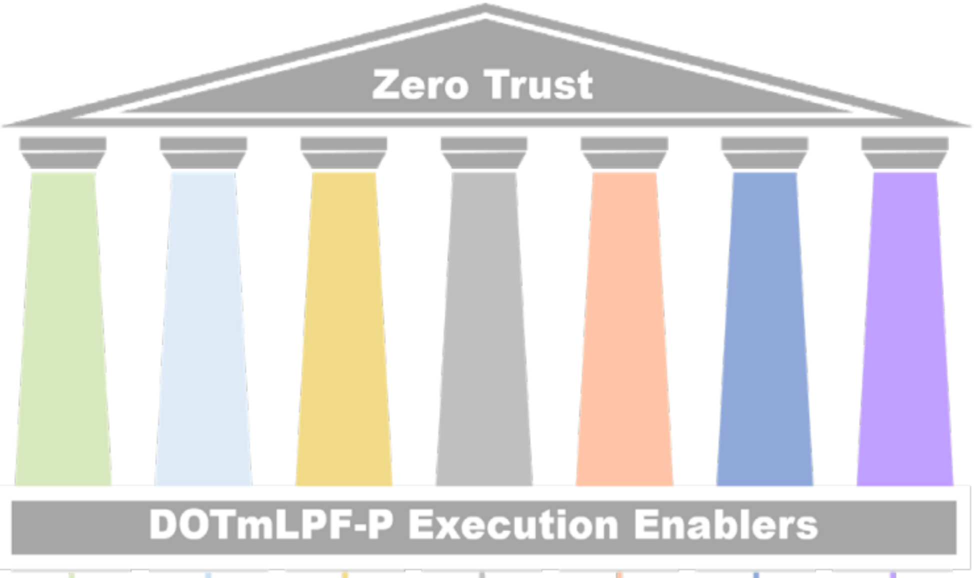
Late 2024

DON must transition to a ZT cybersecurity framework for networks and implement ICAM by end of fiscal 2027

GOAL: DON is ZT compliant by 2030

Slide adapted from a presentation by Mr. David Voelker, DON CIO Zero Trust Lead

DoD Zero Trust Capability Pillars



User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Applications & Workloads

Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.

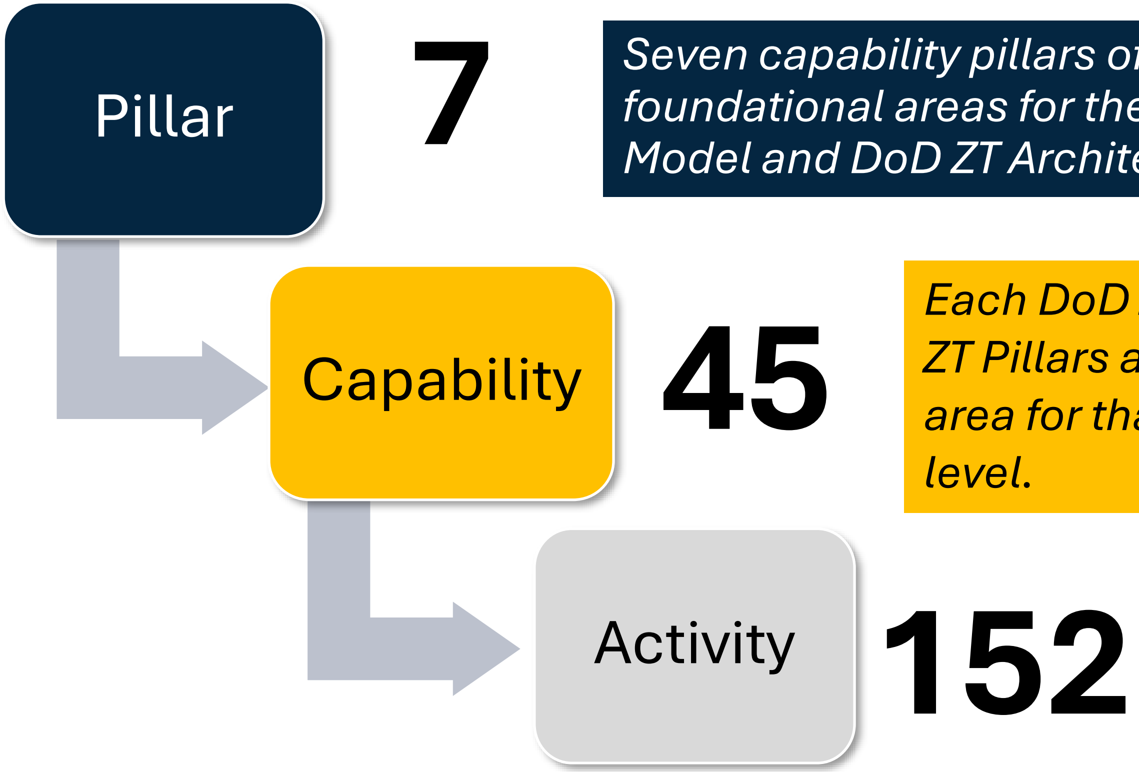
Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Zero Trust Pillars, Capabilities, and Activities



Pillar

7

Seven capability pillars of Zero Trust that provide the foundational areas for the DoD Zero Trust Security Model and DoD ZT Architectures

Capability

45

Each DoD ZT Capability aligns to one of the seven DoD ZT Pillars and represents a more in-depth measurement area for that specific Pillar at the Target or Advanced level.

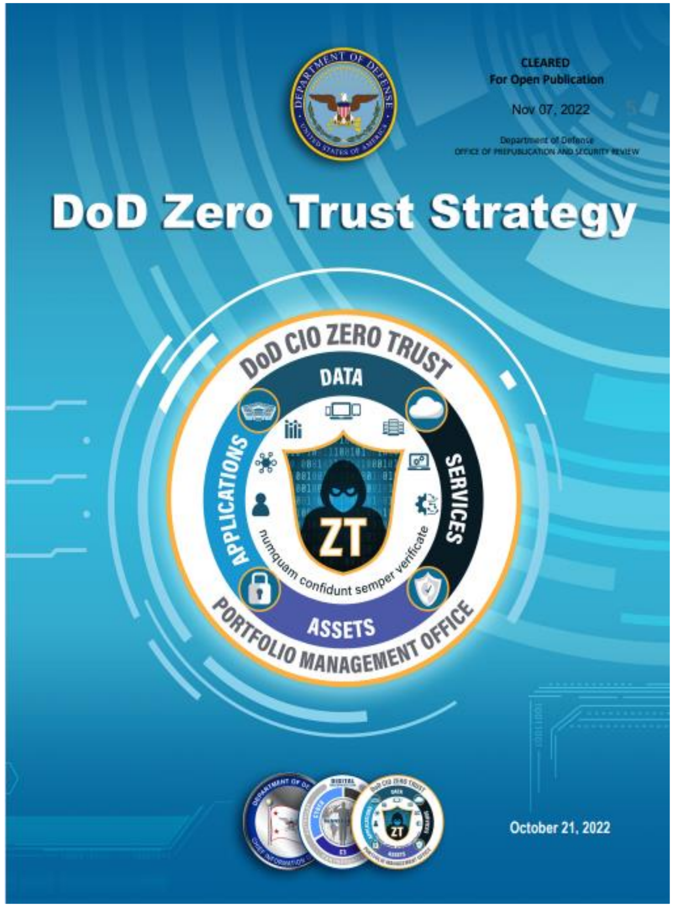
Activity

152

Capabilities break down into activities with associated ZT Phases or Levels to better support appropriate sequencing and recognize predecessor and successor relationships. *There are 91 Target Level and 61 Advanced Level Activities*

Target ZT: All DoD organizations must achieve this level
Advanced ZT: Certain organizations must reach this level based on system and information sensitivity

Major ZT Imperatives for DoD Components



CLEARED
For Open Publication
Nov 07, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Zero Trust Strategy

October 21, 2022

DoD CIO ZERO TRUST
DATA
APPLICATIONS
SERVICES
ZT
numquam confidunt semper verificate
ASSETS
PORTFOLIO MANAGEMENT OFFICE

1 *Demonstrate "Target levels" of Zero Trust*

2 *Conduct regular assessments of their Zero Trust implementation*

3 *Develop and implement Zero Trust roadmaps and plans*

4 *Adopt and integrate Zero Trust capabilities, technologies, solutions, and processes*

Problem Statement for the DON

The DON needs a solution to track and communicate ZT implementation plan progress across **1,500+ DON programs, systems, applications, and networks** in a standardized way *(and make it easy for leadership to review status in real time)*

DON CDAO Functional Areas

Architecture

Develop and maintain a strong connection to mission and technical implementation through a data-driven architecture

Governance & Oversight

Develop, coordinate, and enforce data policy and processes

Enterprise Data, Analytics, AI Services

Support the Naval Enterprise Data and Analytics Environment as part of a broader suite of Enterprise Services to ensure maximal use of data

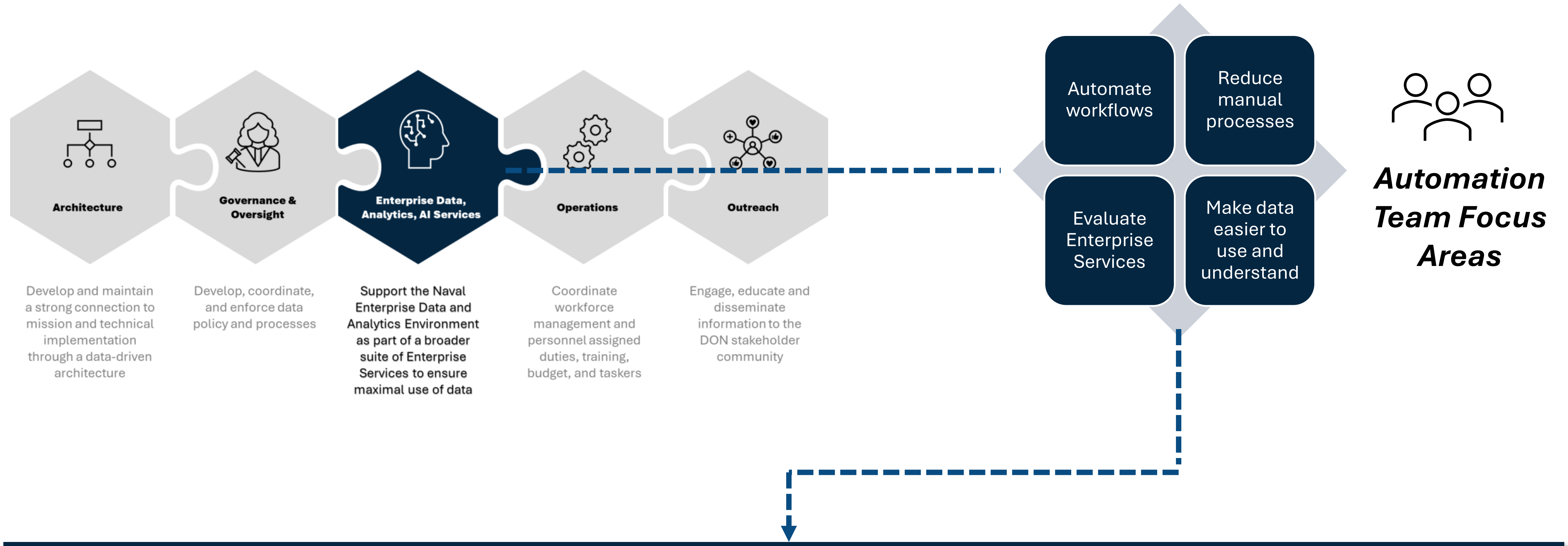
Operations

Coordinate workforce management and personnel assigned duties, training, budget, and taskers

Outreach

Engage, educate and disseminate information to the DON stakeholder community

DON CDAO Automation Team



Architecture

Develop and maintain a strong connection to mission and technical implementation through a data-driven architecture

Governance & Oversight

Develop, coordinate, and enforce data policy and processes

Enterprise Data, Analytics, AI Services

Support the Naval Enterprise Data and Analytics Environment as part of a broader suite of Enterprise Services to ensure maximal use of data

Operations

Coordinate workforce management and personnel assigned duties, training, budget, and taskers

Outreach

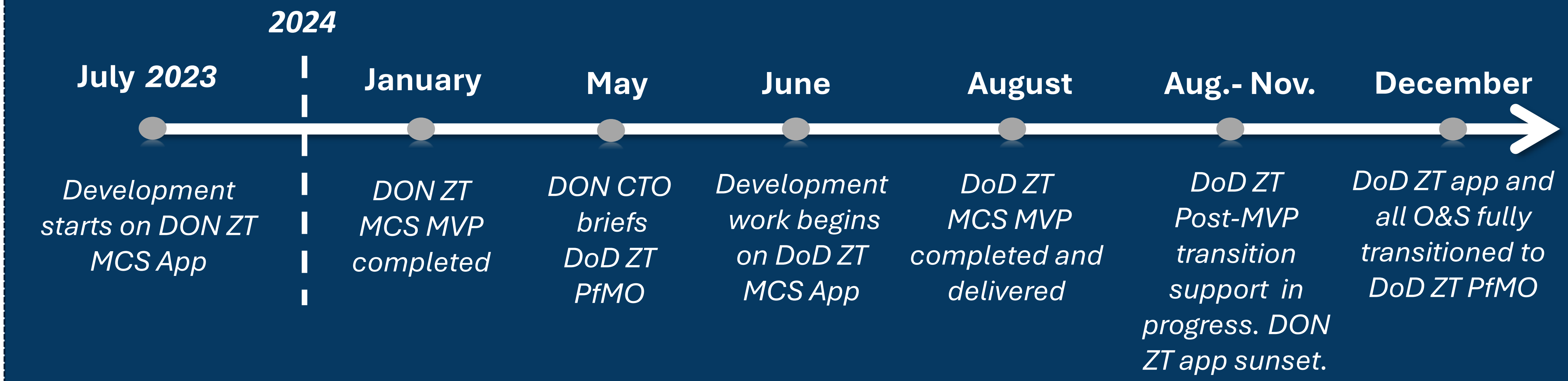
Engage, educate and disseminate information to the DON stakeholder community

Automate workflows	Reduce manual processes
Evaluate Enterprise Services	Make data easier to use and understand

Automation Team Focus Areas

This effort presented a unique opportunity for the DON CDAO Automation Team to support overall DON ZT implementation objectives in coordination with DON CISO and DoD ZT PfMO

ZT MCS High-Level Development Timeline



2024

July 2023 – Development starts on DON ZT MCS App

January – DON ZT MCS MVP completed

May – DON CTO briefs DoD ZT PfMO

June – Development work begins on DoD ZT MCS App

August – DoD ZT MCS MVP completed and delivered

Aug.- Nov. – DoD ZT Post-MVP transition support in progress. DON ZT app sunset.

December – DoD ZT app and all O&S fully transitioned to DoD ZT PfMO

DON Approach to Capturing ZT status

Approach

- Provide user-friendly web application with a SharePoint or database back-end
- Request the same information contained in the spreadsheets developed by DoD ZT PfMO
- Require quarterly responses / updates for the 91 Target level activities and 61 Advanced activities (if applicable)
- Create app that reduces manual inputs and provide visibility and real-time status updates to leadership via dashboards

Benefit

- **Allows Components to update on their schedule**
- **Provides method to track inheritance pathway between Parent and Child programs**
- **Captures previously entered information so organizations only need to update changes (deltas) after initial entry**
- **Provides a common data set that meets the reporting needs for multiple echelons**
- **Data can be visualized in real-time to show the DON's progress towards meeting the DoD Zero Trust deadline**

ZT-MCS Simplified Data Model

System

Capture Data: Users enter information about Network, Device, System, etc.

Status

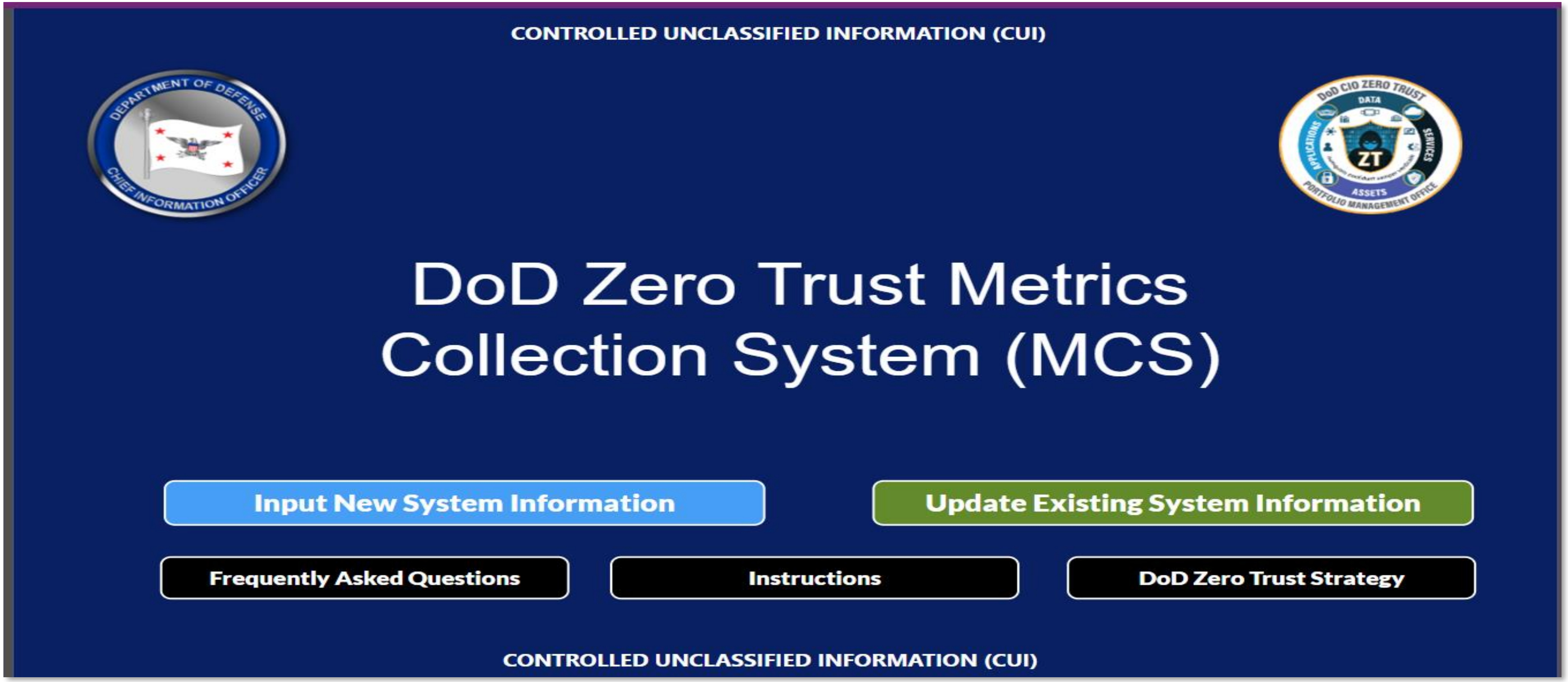
Capture Data: Users enter Zero Trust information for each of the Activities

Activity

Lookup Data: Provides information about each Activity, including Phase, Pillar, Name, Desc.

Three SharePoint Lists operate as integrated data tables that power the ZT-MCS application

DON ZT MCS Overview



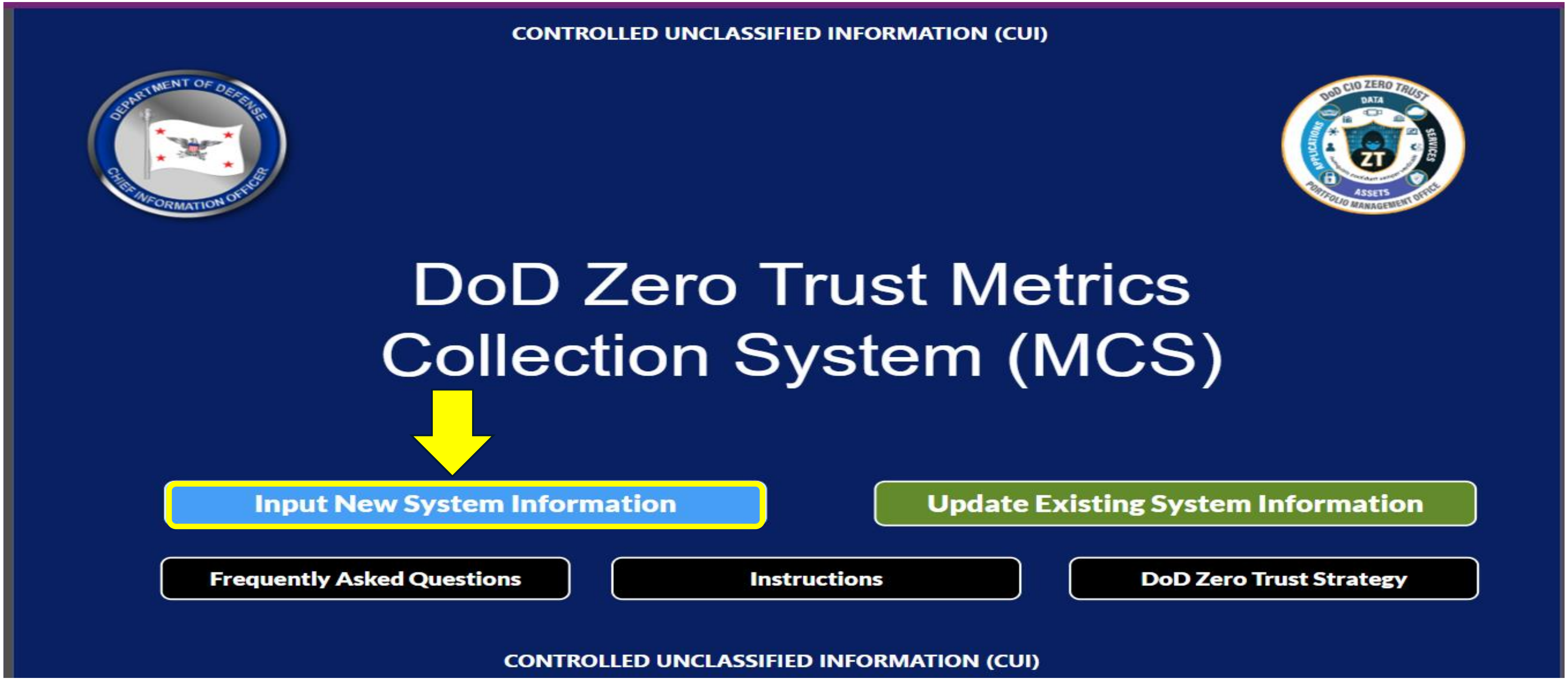
CONTROLLED UNCLASSIFIED INFORMATION (CUI)

DoD Zero Trust Metrics Collection System (MCS)

Input New System Information
Update Existing System Information
Frequently Asked Questions
Instructions
DoD Zero Trust Strategy

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Input New System Information



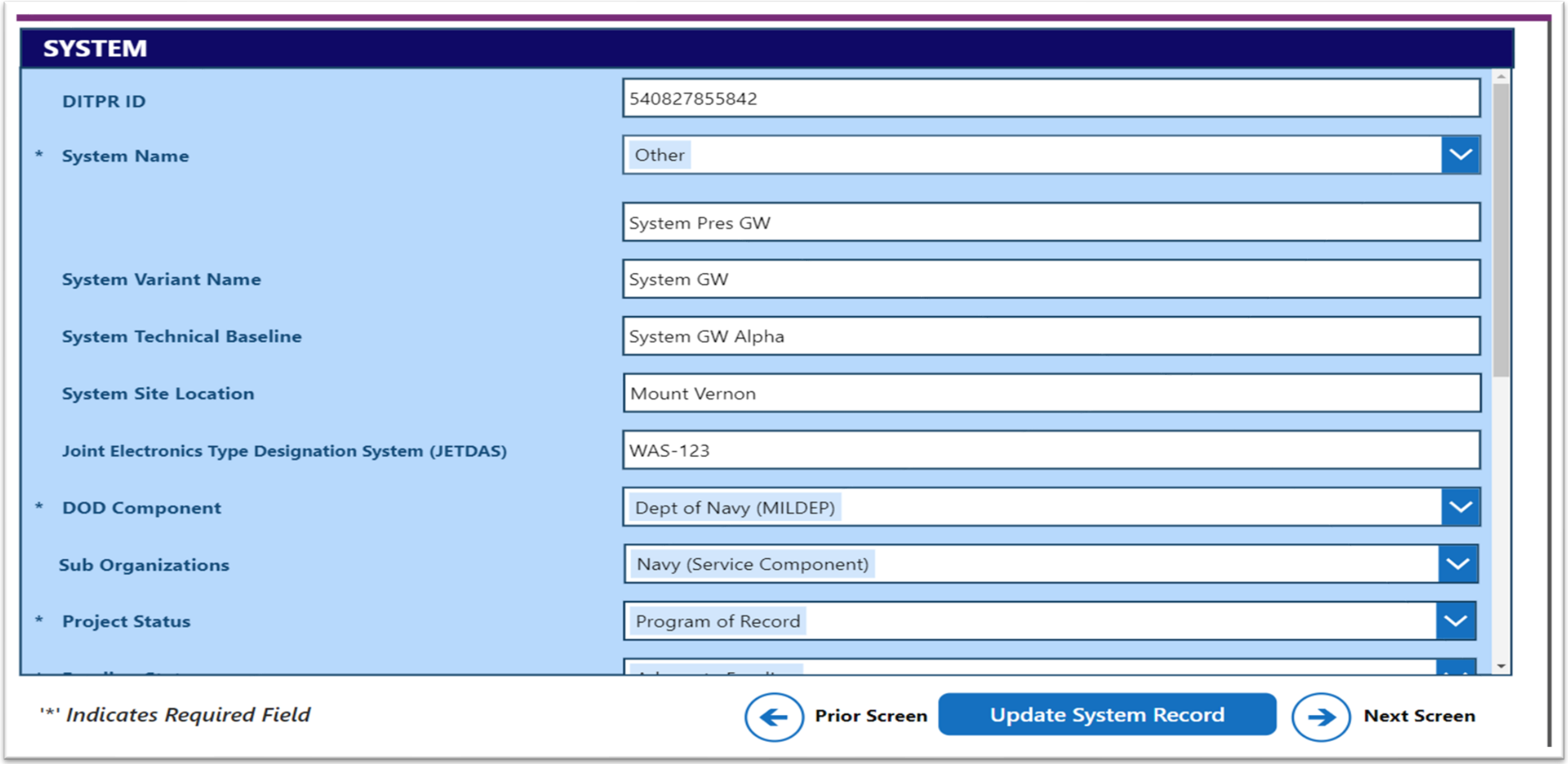
CONTROLLED UNCLASSIFIED INFORMATION (CUI)

DoD Zero Trust Metrics Collection System (MCS)

Input New System Information
Update Existing System Information
Frequently Asked Questions
Instructions
DoD Zero Trust Strategy

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

System Screen

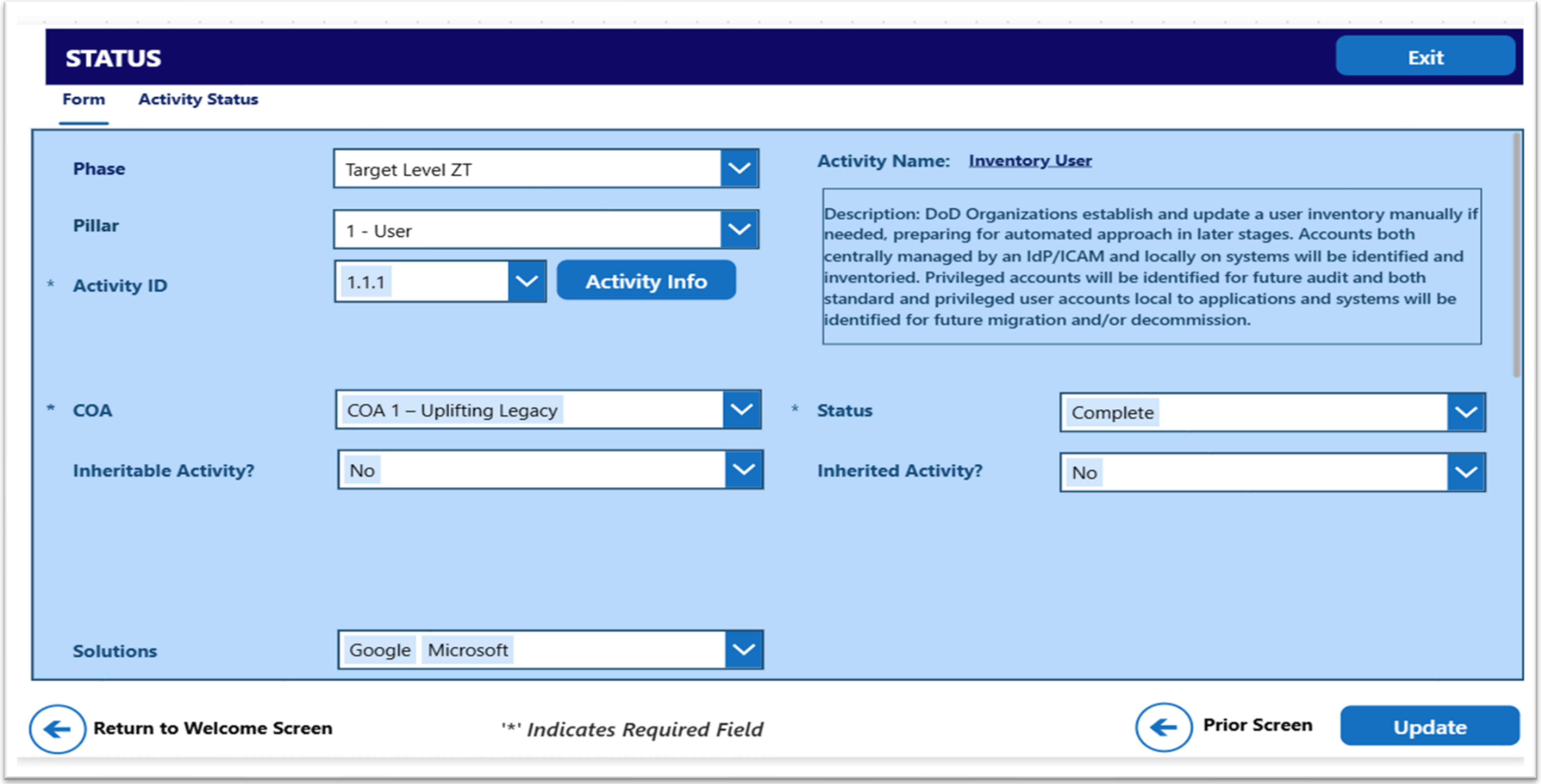


SYSTEM

DITPR ID	540827855842
* System Name	Other
	System Pres GW
System Variant Name	System GW
System Technical Baseline	System GW Alpha
System Site Location	Mount Vernon
Joint Electronics Type Designation System (JETDAS)	WAS-123
* DOD Component	Dept of Navy (MILDEP)
Sub Organizations	Navy (Service Component)
* Project Status	Program of Record

'*' *Indicates Required Field*

Status Screen



STATUS

Phase: Target Level ZT

Pillar: 1 - User

* Activity ID: 1.1.1

Activity Name: Inventory User

Description: DoD Organizations establish and update a user inventory manually if needed, preparing for automated approach in later stages. Accounts both centrally managed by an IdP/ICAM and locally on systems will be identified and inventoried. Privileged accounts will be identified for future audit and both standard and privileged user accounts local to applications and systems will be identified for future migration and/or decommission.

* COA: COA 1 – Uplifting Legacy

* Status: Complete

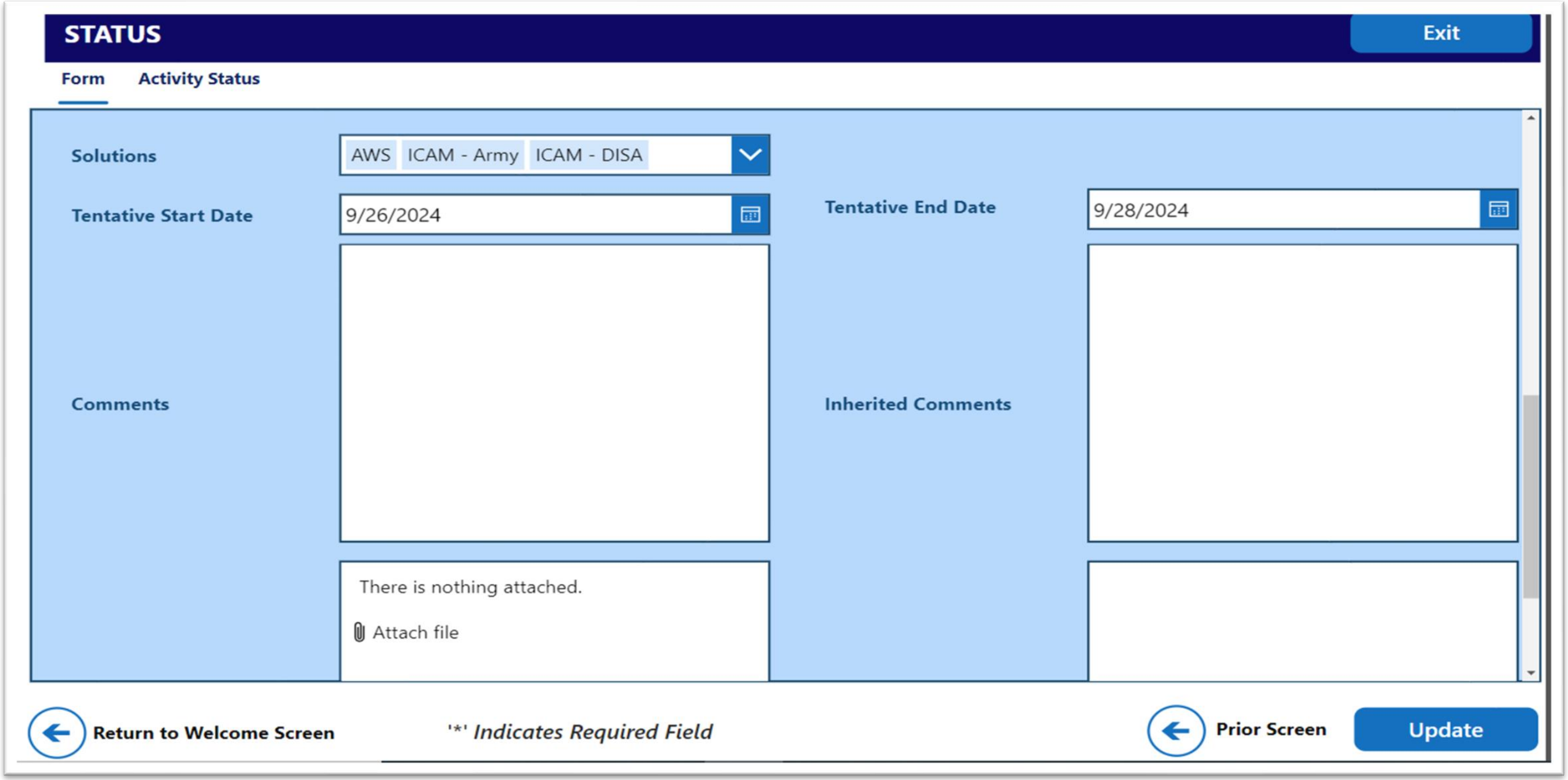
Inheritable Activity?: No

Inherited Activity?: No

Solutions: Google Microsoft

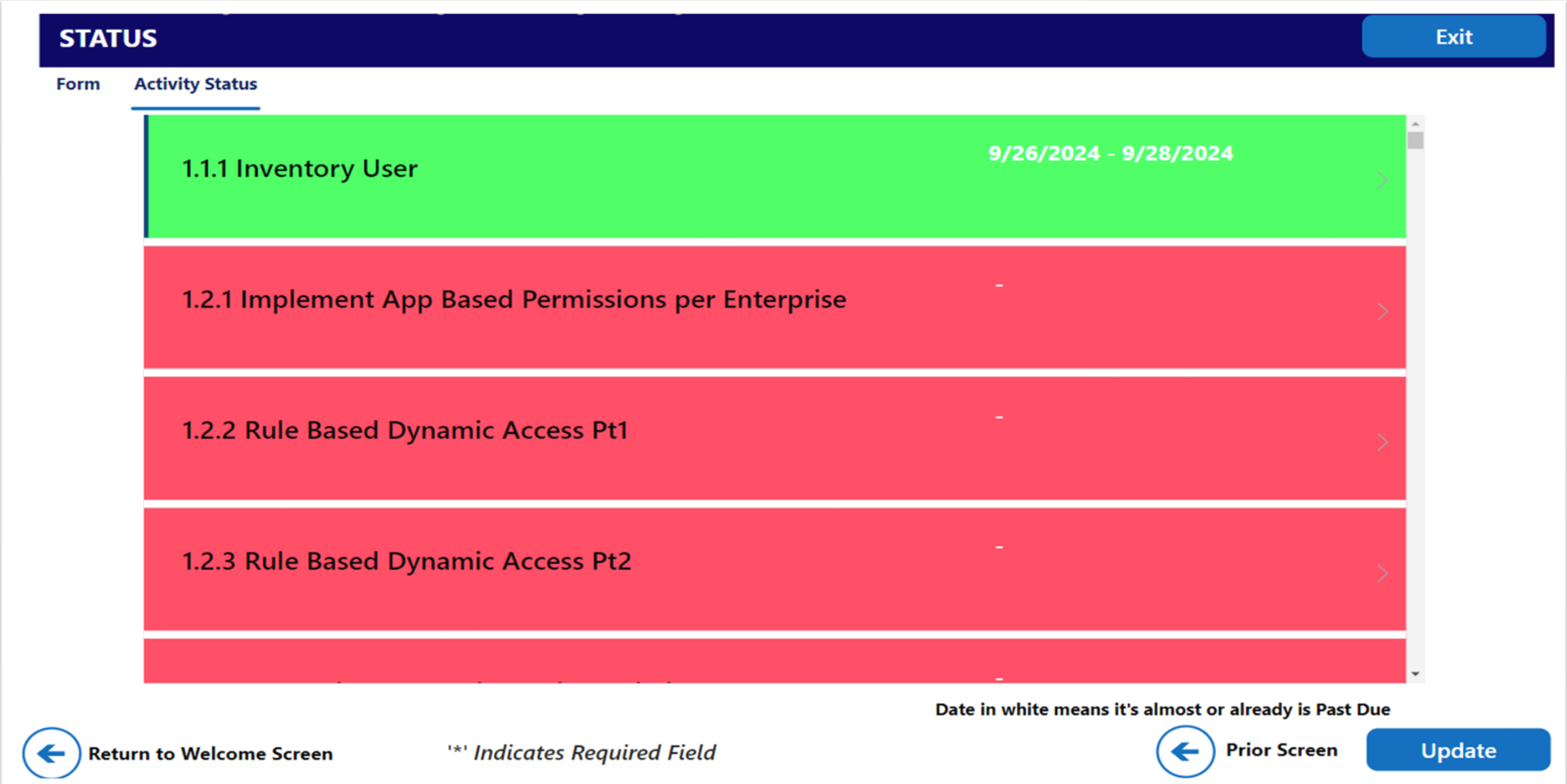
'*' *Indicates Required Field*

Status Screen (Cont’d.)



Solutions	AWS ICAM - Army ICAM - DISA		
Tentative Start Date	9/26/2024	Tentative End Date	9/28/2024
Comments		Inherited Comments	
	There is nothing attached. Attach file		

Activity Status Tracker

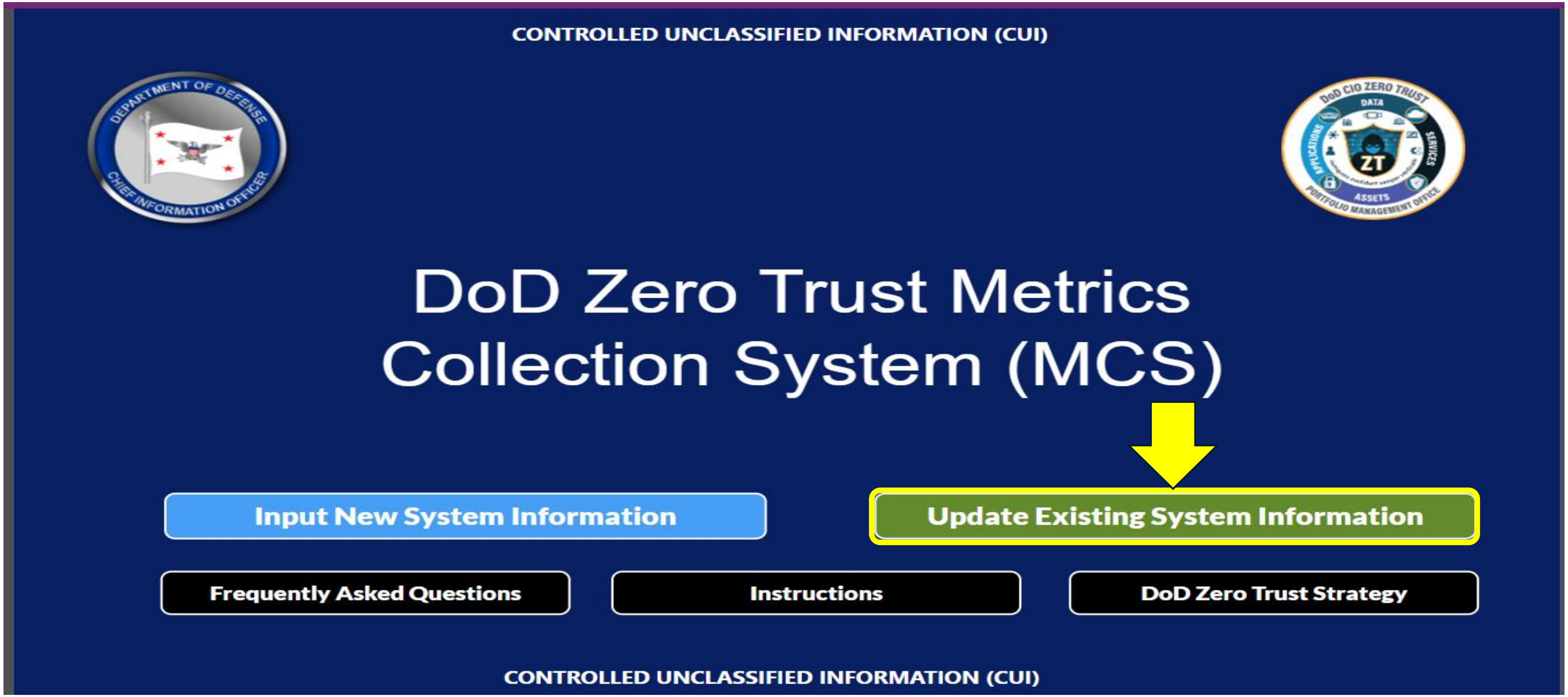


1.1.1 Inventory User	9/26/2024 - 9/28/2024
1.2.1 Implement App Based Permissions per Enterprise	-
1.2.2 Rule Based Dynamic Access Pt1	-
1.2.3 Rule Based Dynamic Access Pt2	-

Date in white means it's almost or already is Past Due

'*' *Indicates Required Field*

Input New System Information



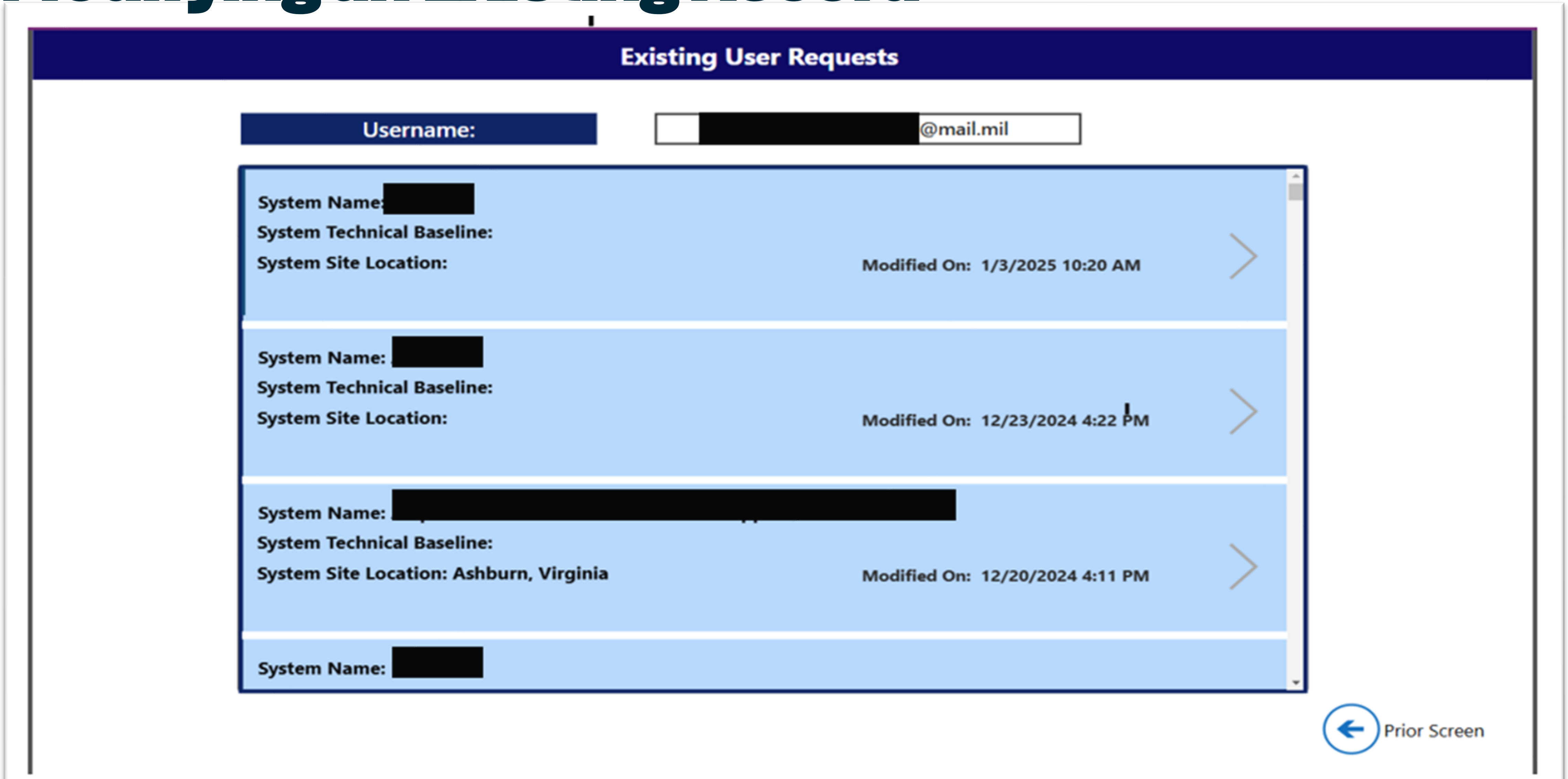
CONTROLLED UNCLASSIFIED INFORMATION (CUI)

DoD Zero Trust Metrics Collection System (MCS)

Input New System Information
Update Existing System Information
Frequently Asked Questions
Instructions
DoD Zero Trust Strategy

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Modifying an Existing Record



Existing User Requests

Username: [redacted]@mail.mil

System Name: [redacted]
System Technical Baseline:
System Site Location:
Modified On: 1/3/2025 10:20 AM

System Name: [redacted]
System Technical Baseline:
System Site Location:
Modified On: 12/23/2024 4:22 PM

System Name: [redacted]
System Technical Baseline:
System Site Location: Ashburn, Virginia
Modified On: 12/20/2024 4:11 PM

System Name: [redacted]

Key Features and Takeaways

Speed

Six months to deliver an operational DON app and an additional four months for DoD development

Security

Information is stored in OSD DISA IL5 SharePoint, not viewable to other users and can be easily transferred to Advana

Low-Cost

Utilizes existing NIPR O365 capabilities with no additional needs for subscriptions or software

Low-Code

Easy-to-understand drop-downs / code that is easily portable and transferrable across teams and developers

Accessibility

Can be accessed by most DoD Components with a CAC

Insights

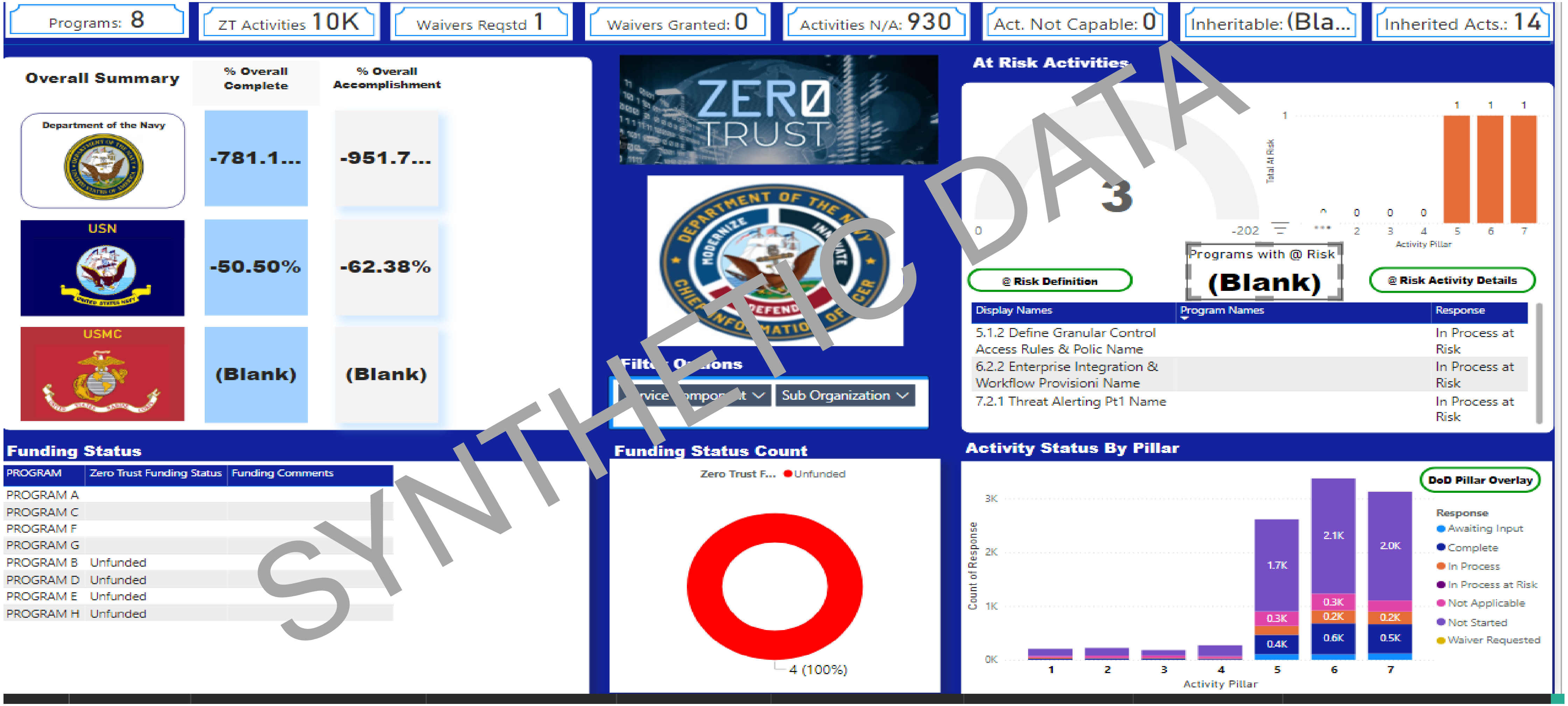
Dashboard visualizations provide insight into Component ZT progress, including status, courses of action, tools used, and inheritance

DON CIO

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

Optimize | Secure | decide

DON ZT MCS Dashboard



Programs: 8 | ZT Activities 10K | Waivers Reqstd 1 | Waivers Granted: 0 | Activities N/A: 930 | Act. Not Capable: 0 | Inheritable: (Bla... | Inherited Acts.: 14

Overall Summary	% Overall Complete	% Overall Accomplishment
Department of the Navy	-781.1...	-951.7...
USN	-50.50%	-62.38%
USMC	(Blank)	(Blank)

Filter Options

rvice ompon t ⌄ | Sub Organization ⌄

At Risk Activities

Programs with @ Risk
(Blank)

Display Names	Program Names	Response
5.1.2 Define Granular Control Access Rules & Polic Name		In Process at Risk
6.2.2 Enterprise Integration & Workflow Provisioni Name		In Process at Risk
7.2.1 Threat Alerting Pt1 Name		In Process at Risk

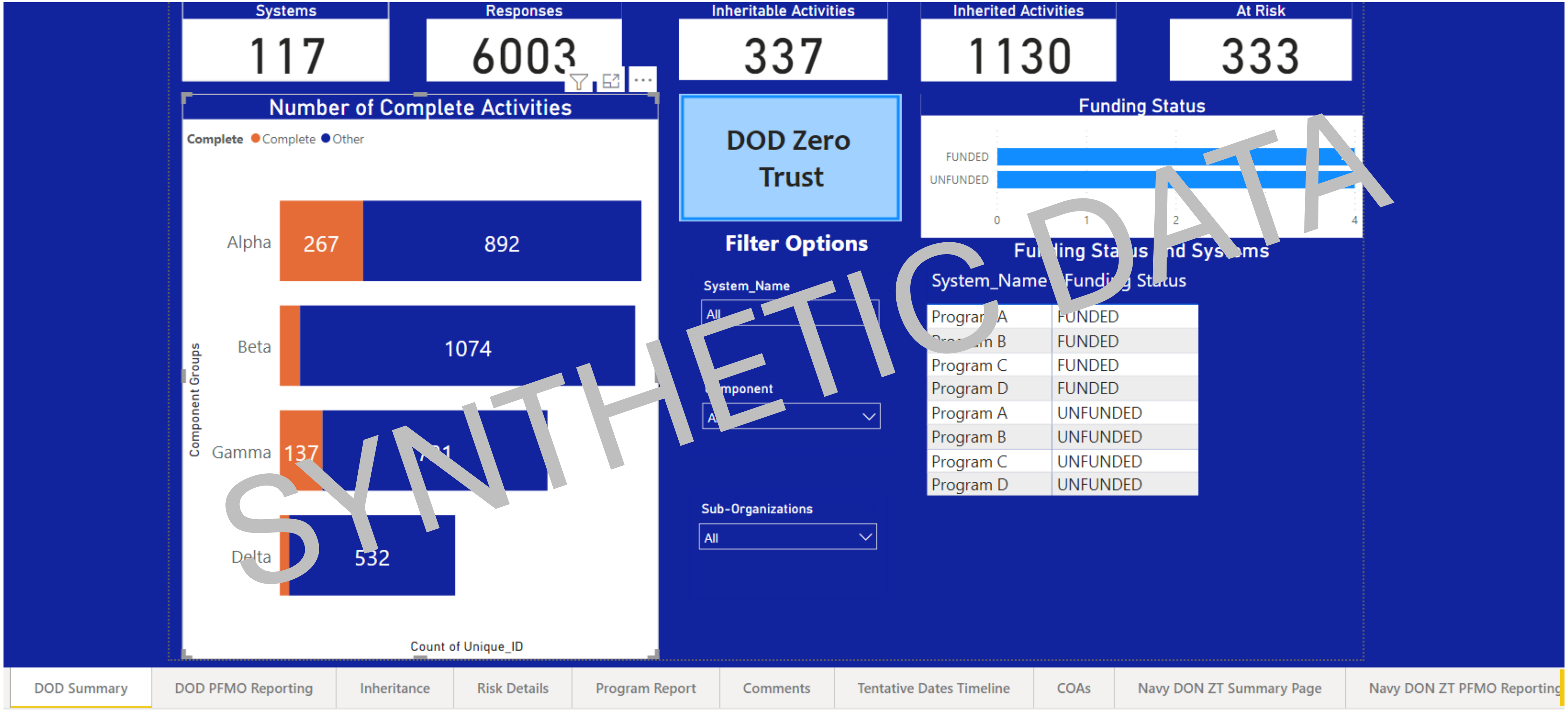
Funding Status

PROGRAM	Zero Trust Funding Status	Funding Comments
PROGRAM A		
PROGRAM C		
PROGRAM F		
PROGRAM G		
PROGRAM B	Unfunded	
PROGRAM D	Unfunded	
PROGRAM E	Unfunded	
PROGRAM H	Unfunded	

Funding Status Count

Activity Status By Pillar

DoD ZT MCS Dashboard



Systems	Responses	Inheritable Activities	Inherited Activities	At Risk
117	6003	337	1130	333

Number of Complete Activities

DOD Zero Trust

Filter Options

System_Name
All

Component
All

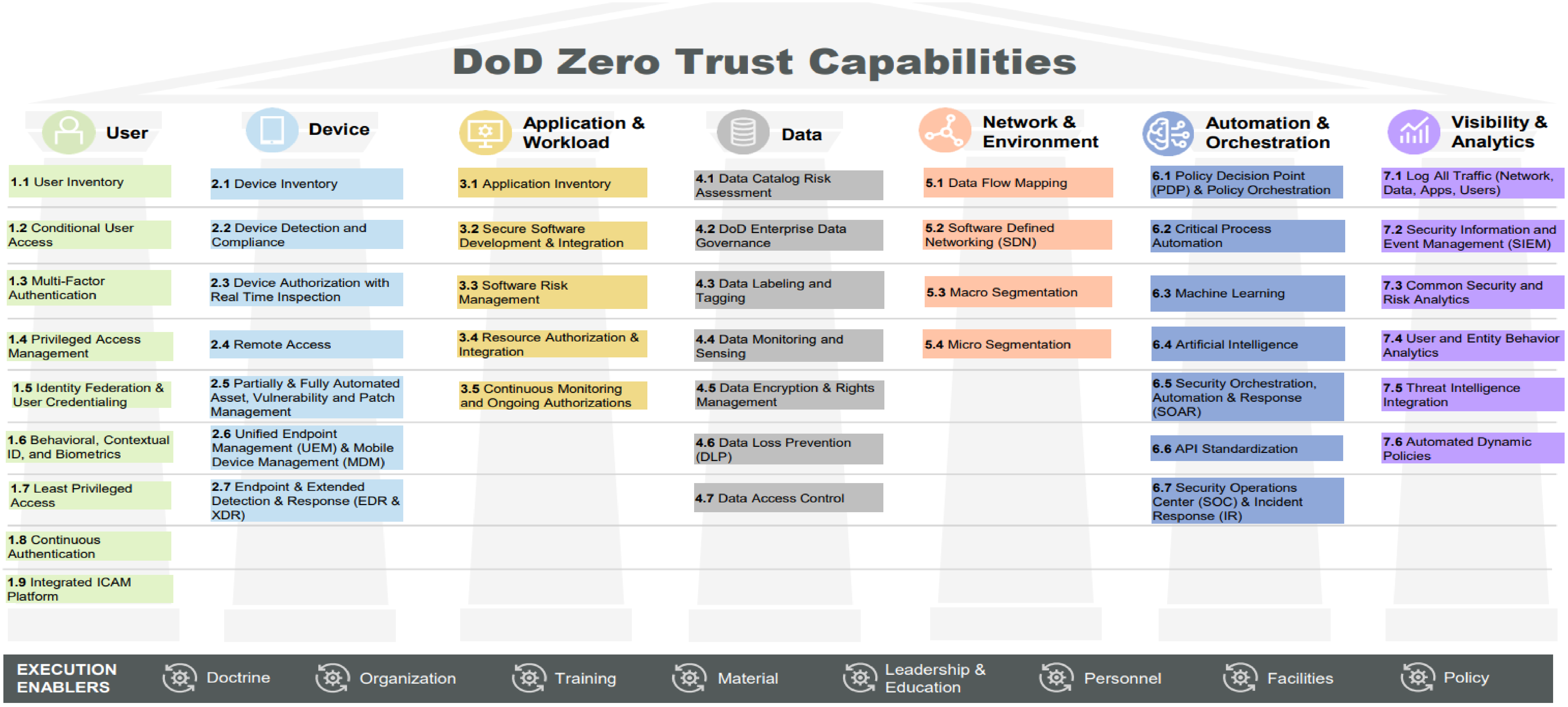
Sub-Organizations
All

Funding Status

Funding Status and Systems

System_Name	Funding Status
Program A	FUNDED
Program B	FUNDED
Program C	FUNDED
Program D	FUNDED
Program A	UNFUNDED
Program B	UNFUNDED
Program C	UNFUNDED
Program D	UNFUNDED

Zero Trust Capabilities



DoD Zero Trust Capabilities

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS Doctrine | Organization | Training | Material | Leadership & Education | Personnel | Facilities | Policy