



Space Systems Command (SSC)
S6 Communications

# ZT Assessments to support Sub I-Plan Templates

## An S6 view to starting the Zero Trust journey

Maj Min Kang, S6 Acting Cybersecurity Division Chief
Chad Korosec, MITRE

# Agenda

## Lexicon

**Context Gaps Undermine Communication**

- Terminology issues are persistent
- Language requires context to resolve

## Self-Evaluation

**S6 ZT Self-Evaluations Framework**

- Self-evaluation history and status
- Design and Usage
- Next Steps

## Use Case

**ZT Assessment with System Owner**

- Assessment Overview
- Lessons Learned
- SSC/S6 Takeaways

# A Quick Detour: Terminology

Terminology issues are persistent; they require context to resolve

## EIT Systems

Most Systems on NIPRNet, SIPRNet and Cloud

## Non-EIT Systems

Weapon Systems, Mission Systems, Industrial Control Systems, Defense Critical Infrastructure, and Operational Technology

Source: DAF I-Plan v.2 Draft, 1 Mar 25

# Lexicon of Non-EIT

## A reoccurring theme is communication regarding Non-EIT systems:

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| **Operational Technology (OT)** | Hardware/software that monitors and controls physical systems in real-time | Real-world actuation and sensing | Encompasses ICS and embedded control in platforms | HVAC systems, shipboard power, flightline logistics & maintenance | Availability, safety, physical-layer hardening |
| Weapon Systems | | | | | |
| *Mission Systems* | | | | | |
| Defense Critical Infrastructure (DCI) | | | | | |
| Industrial Control Systems (ICS) | | | | | |

Source: See Page Notes

# Lexicon of Non-EIT

A reoccurring theme is communication regarding Non-EIT systems:

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| Operational Technology (OT) | | | | | |
| **Weapon Systems** | Systems designed to apply lethal or non-lethal force to achieve combat effects | Engage and neutralize adversaries | Combat platforms and subsystems | F-35, M1 Abrams, Patriot System, Tomahawk | Mission assurance, survivability, confidentiality/integrity |
| *Mission Systems* | | | | | |
| Defense Critical Infrastructure (DCI) | | | | | |
| Industrial Control Systems (ICS) | | | | | |

Source: See Page Notes

# Lexicon of Non-EIT

## A reoccurring theme is communication regarding Non-EIT systems:

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| Operational Technology (OT) | | | | | |
| Weapon Systems | | | | | |
| ***Mission Systems*** | *Systems that support military operations (C2, ISR, navigation, targeting) but do not directly deliver kinetic effects* | *Enable operational decisions and coordination* | *Embedded or standalone systems* | *Aegis system, AWACS sensors, GPS receivers, C2 nodes* | *Availability, integrity, confidentiality* |
| Defense Critical Infrastructure (DCI) | | | | | |
| Industrial Control Systems (ICS) | | | | | |

Source: See Page Notes

# Lexicon of Non-EIT

## A reoccurring theme is communication regarding Non-EIT systems:

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| Operational Technology (OT) | | | | | |
| Weapon Systems | | | | | |
| *Mission Systems* | | | | | |
| **Defense Critical Infrastructure (DCI)** | Assets and systems essential to DoD missions, often owned by private sector or other agencies | Sustain DoD operational capability | Facilities, utilities, supply chains, telecoms | Defense industrial base, electric grid, SATCOM, energy | Resilience, interdependency risk, continuity of operations |
| Industrial Control Systems (ICS) | | | | | |

Source: See Page Notes

# Lexicon of Non-EIT

A reoccurring theme is communication regarding Non-EIT systems:

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| Operational Technology (OT) | | | | | |
| Weapon Systems | | | | | |
| *Mission Systems* | | | | | |
| Defense Critical Infrastructure (DCI) | | | | | |
| **Industrial Control Systems (ICS)** | Systems that monitor/control industrial processes in facilities and platforms | Automate physical infrastructure and logistics | Subset of OT focused on process automation | SCADA, PLCs, DCS in water/power/fuel depots | Safety, availability, secure remote access |

Source: See Page Notes

# Lexicon of Non-EIT

## Most communications in USSF land on Mission System (but require context):

| Category | Definition | Primary Purpose | Scope | Examples | Security Focus |
|---|---|---|---|---|---|
| **Operational Technology (OT)** | Hardware/software that monitors and controls physical systems in real-time | Real-world actuation and sensing | Encompasses ICS and embedded control in platforms | HVAC systems, shipboard power, flightline logistics & maintenance | Availability, safety, physical-layer hardening |
| **Weapon Systems** | Systems designed to apply lethal or non-lethal force to achieve combat effects | Engage and neutralize adversaries | Combat platforms and subsystems | F-35, M1 Abrams, Patriot System, Tomahawk | Mission assurance, survivability, confidentiality/integrity |
| ***Mission Systems*** | *Systems that support military operations (C2, ISR, navigation, targeting) but do not directly deliver kinetic effects* | *Enable operational decisions and coordination* | *Embedded or standalone systems* | *Aegis system, AWACS sensors, GPS receivers, C2 nodes* | *Availability, integrity, confidentiality* |
| **Defense Critical Infrastructure (DCI)** | Assets and systems essential to DoD missions, often owned by private sector or other agencies | Sustain DoD operational capability | Facilities, utilities, supply chains, telecoms | Defense industrial base, electric grid, SATCOM, energy | Resilience, interdependency risk, continuity of operations |
| **Industrial Control Systems (ICS)** | Systems that monitor/control industrial processes in facilities and platforms | Automate physical infrastructure and logistics | Subset of OT focused on process automation | SCADA, PLCs, DCS in water/power/fuel depots | Safety, availability, secure remote access |

Source: See Page Notes

# SSC/S6 ZT Self-Evaluation Framework

# Zero Trust Self-Evaluation Goals and Objectives

## Goal

Develop a tool/framework to assist with DoD ZT Capability assessment

## Data Discovery

Assist system owners in ZT assessments; focus on identifying areas where S6 can best assist systems across the enterprise

## Framework

Tool to capture the DoD ZT capability section of the Sub I-Plan template

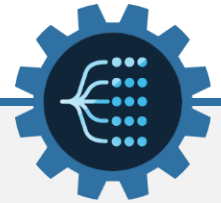
- Encapsulates all target activities to inform the 34 basic capabilities

# Past 6-months of ZT Focus for SSC/S6

Track DAF and DoD ZT Efforts

Create a Self-Evaluation Framework for Systems Owners

Coordinate with Systems Owners to Validate Self-Evaluations



Establish Mechanisms to Track and Measure ZT Progress

# What questions drove activities?

- How long will initial ZT assessments take for mission systems?
- What is Included in a ZT assessment?
- How can the S6 help ensure assessments by System Owners?

## SAF/CN

What actions related to Zero Trust are coming down that will impact system owners?

## SSC/S6

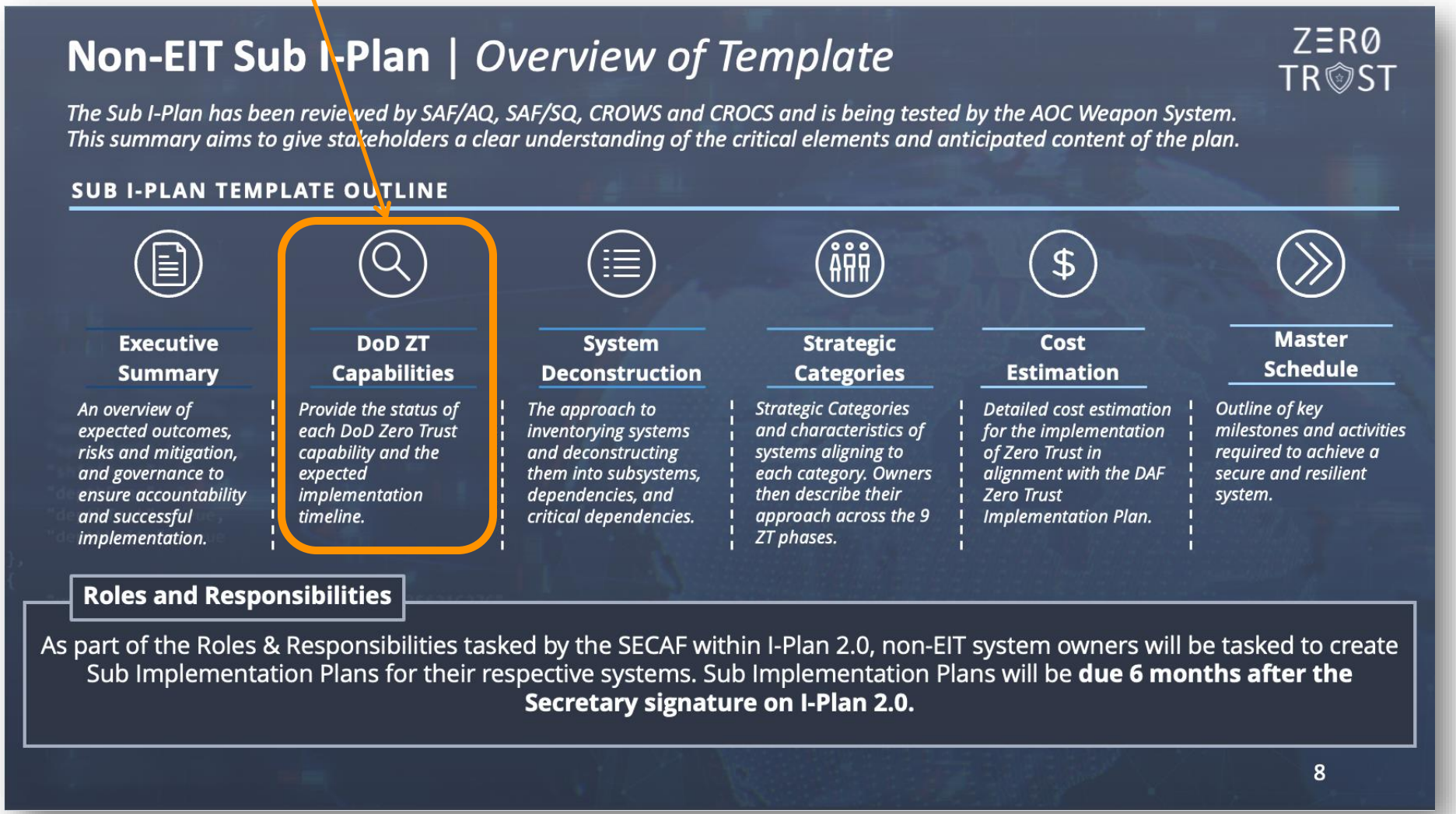
How can the S6 prepare to assist system owners ensure compliance with the ZT mandates?

## SSC/System Owners

What can the S6 provide or assist systems owners with to help reach ZT mandate?

# Core Activity: Sub I-Plan Template Focused

Initial Focus on DoD ZT Capabilities






Source: DAF ZT Sub I-Plan Group Presentation to USSF SSC Cyber Expo

# S6 ZT Self-Evaluation Framework

## The Process

- Framework to guide system owners through assessment
- Map out by pillar; adapt to DAF Sub I-Plan Template as needed

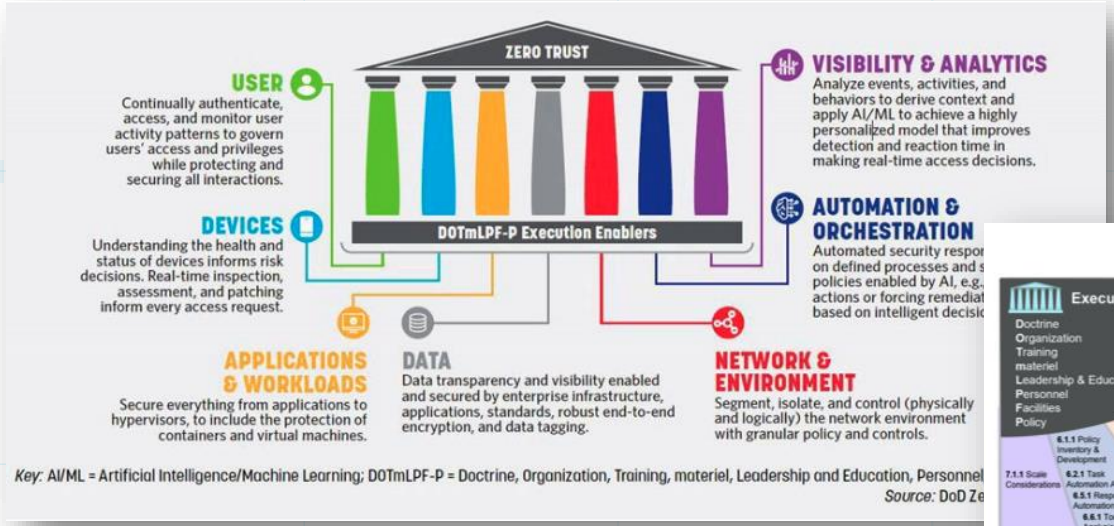
## The Product

- Develop in Excel for ease of use/sharing
- Layout by Pillar
- Allow Excel functions to aid users

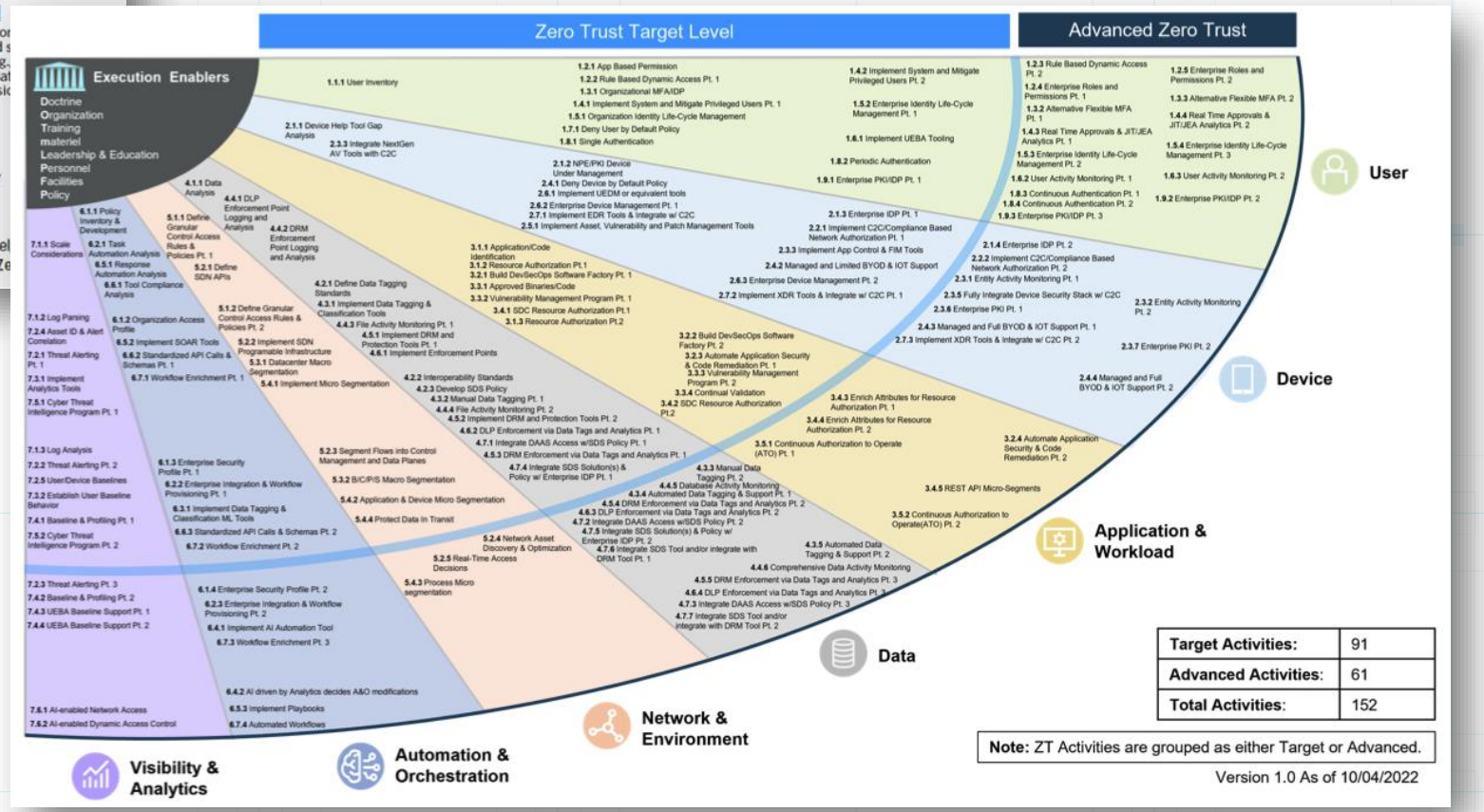
## The Future

- Adapt as required for future use

# Detour: Level of Detail




Activities mapped by pillar




Focused on Target Activities

Source: DoD Zero Strategy, 21 Oct 2022

# Informing the Self-Evaluation


[Insert classification level]

Department of the Air Force
Zero Trust
Sub Implementation Plan

ZERO TRUST

[Insert system name] Sub Implementation Plan

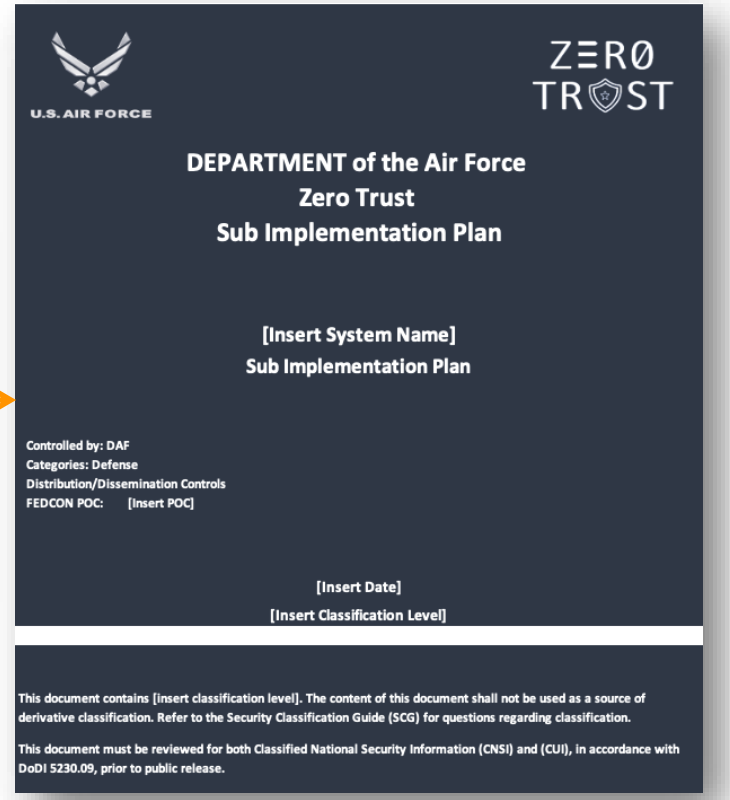
Controlled by: DAF
Categories: Defense
Distribution/Dissemination Controls
FEDCON POC:

[Insert Date]
[Insert Classification Level]

Source: DAF ZT Sub I-Plan Template DOC Format

Focus is on analysis of ZT Capabilities

| DoD ZT Capabilities | | | |
|---|---|---|---|
| **Capability** | **Status** | **Expected Implementation Timeline** | **Notes** |
| 1.1 User Inventory | Choose an item. | | Choose an item. |
| 1.2 Conditional User Access | Choose an item. | | Choose an item. |
| 1.3 Multifactor Authentication | Choose an item. | | Choose an item. |
| 1.4 Privileged Access Mgmt. | Choose an item. | | Choose an item. |


U.S. AIR FORCE

ZERO TRUST

DEPARTMENT of the Air Force
Zero Trust
Sub Implementation Plan

[Insert System Name]
Sub Implementation Plan

Controlled by: DAF
Categories: Defense
Distribution/Dissemination Controls
FEDCON POC: [Insert POC]

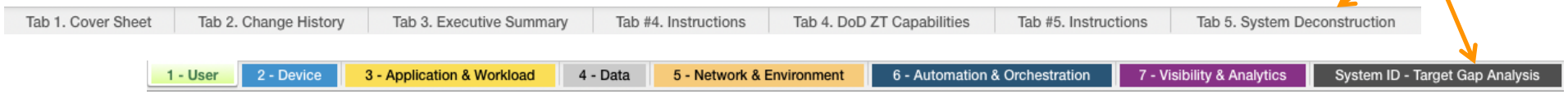
[Insert Date]
[Insert Classification Level]

This document contains [insert classification level]. The content of this document shall not be used as a source of derivative classification. Refer to the Security Classification Guide (SCG) for questions regarding classification.

This document must be reviewed for both Classified National Security Information (CNSI) and (CUI), in accordance with DoDI 5230.09, prior to public release.

Source: DAF ZT Sub I-Plan Template PPTX

Most recent DAF version replicated



# SSC/S6 Self-Evaluation Framework

Excel workbook with various worksheets

Inclusive of DAF Sub I-Plan Template

Based on target activities across the 7 ZT Pillars

Potential updates pending to include advanced activities

# SSC/S6 ZT Self-Evaluation Framework Overview

# Up-Front Matter


U.S. AIR FORCE

ZERO TRUST

**DEPARTMENT of the Air Force**
**Zero Trust**
**Sub Implementation Plan**

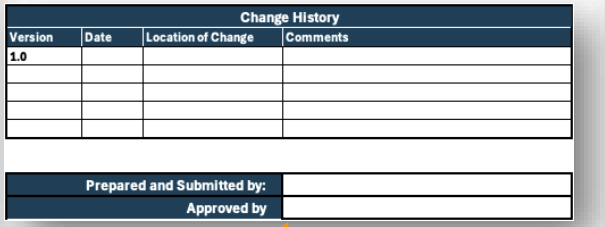
**[Insert System Name]**
**Sub Implementation Plan**

Controlled by: DAF
Categories: Defense
Distribution/Dissemination Controls
FEDCON POC: [Insert POC]

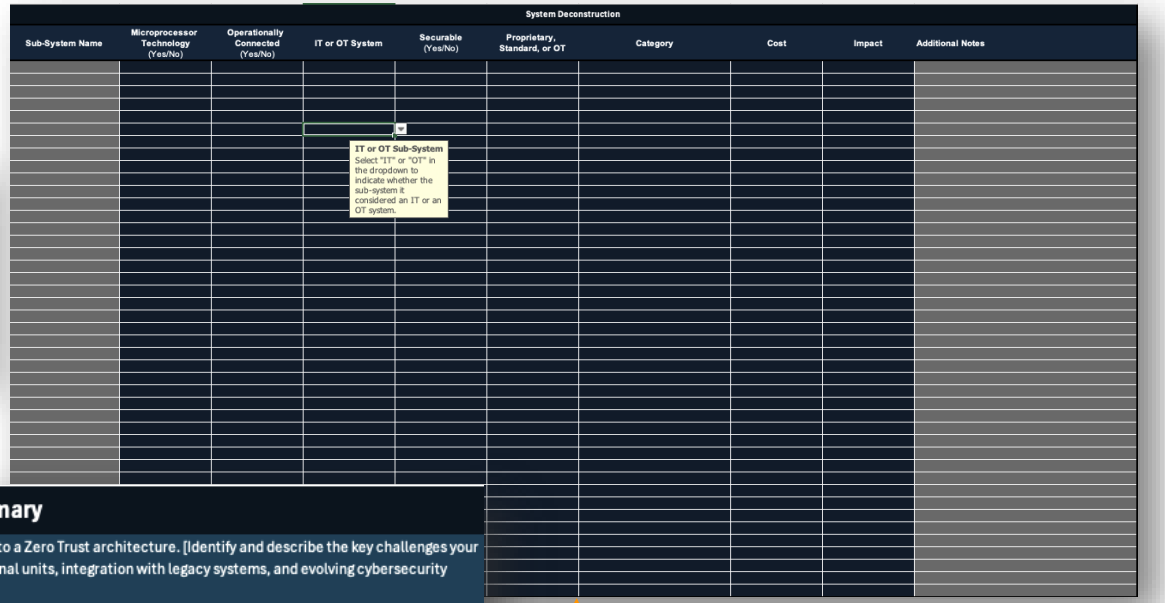
[Insert Date]
[Insert Classification Level]

This document contains [insert classification level]. The content of this document shall not be used as a source of derivative classification. Refer to the Security Classification Guide (SCG) for questions regarding classification.

This document must be reviewed for both Classified National Security Information (CNSI) and (CUI), in accordance with DoDI 5230.09, prior to public release.


| Change History | | | |
|---|---|---|---|
| Version | Date | Location of Change | Comments |
| 1.0 | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | |
|---|---|
| Prepared and Submitted by: | |
| Approved by | |


System Deconstruction

| Sub-System Name | Microprocessor Technology (Yes/No) | Operationally Connected (Yes/No) | IT or OT System | Securable (Yes/No) | Proprietary, Standard, or OT | Category | Cost | Impact | Additional Notes |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

IT or OT Sub-System
Select "IT" or "OT" in the dropdown to indicate whether the sub-system it considered an IT or an OT system.

## Executive Summary

Our organization recognizes the complexity and challenges associated with transitioning to a Zero Trust architecture. [Identify and describe the key challenges your organization anticipates during the implementation such as coordination across operational units, integration with legacy systems, and evolving cybersecurity threats. Discuss how these challenges will be addressed.]

The expected outcomes of our Zero Trust implementation include [Detail the expected outcomes, such as enhanced security posture, improved access controls, and increased resilience against cyber threats. Explain how these outcomes will benefit the organization and align with the DAF Zero Trust Implementation Plan 2.0.]

To achieve these outcomes, we have developed a phased implementation strategy. [Outline the timeframes for each phase, ensuring alignment with the DAF Zero Trust Implementation Plan 2.0. Describe the key milestones and deliverables for each phase.]

High-level risks associated with the implementation include [Identify the high-level risks, such as potential disruptions, integration challenges, and the need for ongoing training and adaptation by personnel. Discuss the mitigation strategies that will be put in place to address these risks.]

To ensure successful implementation, we have established robust governance structures. [Describe the governance structures, including regular oversight mechanisms, communication channels, and defined roles and responsibilities. Explain how these structures will support the implementation process and ensure accountability.]

Tab 1. Cover Sheet | Tab 2. Change History | Tab 3. Executive Summary | Tab #4. Instructions | Tab 4. DoD ZT Capabilities | Tab #5. Instructions | Tab 5. System Deconstruction

Focus of the S6 self-evaluation

Source: DAF ZT Sub I-Plan Template PPTX

# Core Self-Evaluation Framework Content

## Pillar: USER

For additional Capability and ZT Target Information use the '+' signs avove to expand each section

| Responses | Totals | Average |
|---|---|---|
| Not Answered | 3 | 23.08% |
| Not Started | 3 | 23.08% |
| In Process | 3 | 23.08% |
| Complete | 2 | 15.38% |
| N/A | 2 | 15.38% |

N/A and No Responses require a comment

| Number | DoD Zero Trust Capability | ID# | Target Level Activity Name | DOD Target Level Activities Supplemental Info | Clarifying Questions to Identify Activity Intent | Status (Dropdown) | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 1.1 - User Inventory | 1.1.1 | Inventory User | Have the mission areas identified and inventoried regular and privileged users registered in the ICAM system and in local applications, systems, or services that may not yet be integrated with the ICAM system? | Have the mission areas inventoried and cataloged all users within the organization who have or require verified access to the mission system?<br>Have the standard and privileged accounts been identified? | Not Answered | |
| 2 | 1.2 - Conditional User Access | 1.2.1 | Implement App Based Permissions per Enterprise | Have the mission systems established and implemented a standard set of permissions and attributes for each app/resource using the unified enterprise ICAM solution as requirement for subjects seeking access to the app/resource?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add authorization attributes? | Have the mission areas unified and integrated the ICAM solutions using federation where applicable?<br>Have the mission areas established and implemented a standard set of permissions and attributes for each app/resource - using the unified enterprise ICAM solution?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add/specify authorization attributes? | Not Answered<br>Not Started<br>In Process<br>Complete<br>N/A | |
| 3 | 1.2 - Conditional User Access | 1.2.2 | Rule Based Dynamic Access Pt1 | Have the mission systems implemented rule-based dynamic access using user identity and other non-static attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | Have the mission systems implemented rule-based dynamic access using user identity and other attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | In Process | |
| 4 | 1.3 - Multi-Factor Authentication | 1.3.1 | Organizational MFA/IDP | Has the mission system implemented and IdP and MFA solution that is integrated with the enteprise PKI system? | Has the mission system implemented multi-factor authentication, supporting multiple DoD-approved hardware and mobile authenticators to accommodate a wide range of users, devices, partners, mission environments, scenarios, and security access levels?<br>Are the IdP and MFA solutions integrated with the enteprise PKI system? | Complete | |
| 5 | 1.4 - Privileged Access | 1.4.1 | Implement System and Migrate Privileged Users Pt1 | Have you removed of permanent administrator/elevated privileges, implemented a Privileged Account Management (PAM) solution and migrated privileged users to it? Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | Has the mission system removed permanent administrator/elevated privileges, implemented a Privileged Access Management (PAM) system, and migrated privileged users who require access to the PAM user list?<br><br>Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | N/A | |

1 - User | 2 - Device | 3 - Application & Workload | 4 - Data | 5 - Network & Environment | 6 - Automation & Orchestration | 7 - Visibility & Analytics



Source: SSC/S6 ZT Self-Evaluation

# Basic Pillar Worksheet

## Pillar: USER

For additional Capability and ZT Target Information use the '+' signs avove to expand each section

| Responses | Totals | Average |
|---|---|---|
| Not Answered | 3 | 23.08% |
| Not Started | 3 | 23.08% |
| In Process | 3 | 23.08% |
| Complete | 2 | 15.38% |
| N/A | 2 | 15.38% |

N/A and No Responses require a comment

| Number | DoD Zero Trust Capability | ID# | Target Level Activity Name | DOD Target Level Activities Supplemental Info | Clarifying Questions to Identify Activity Intent | Status (Dropdown) | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 1.1 - User Inventory | 1.1.1 | Inventory User | Have the mission areas identified and inventoried regular and privileged users registered in the ICAM system and in local applications, systems, or services that may not yet be integrated with the ICAM system? | Have the mission areas inventoried and cataloged all users within the organization who have or require verified access to the mission system?<br>Have the standard and privileged accounts been identified? | Not Answered | |
| 2 | 1.2 - Conditional User Access | 1.2.1 | Implement App Based Permissions per Enterprise | Have the mission systems established and implemented a standard set of permissions and attributes for each app/resource using the unified enterprise ICAM solution as requirement for subjects seeking access to the app/resource?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add authorization attributes? | Have the mission areas unified and integrated the ICAM solutions using federation where applicable?<br>Have the mission areas established and implemented a standard set of permissions and attributes for each app/resource - using the unified enterprise ICAM solution?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add/specify authorization attributes? | Not Answered<br>Not Started<br>In Process<br>Complete<br>N/A | |
| 3 | 1.2 - Conditional User Access | 1.2.2 | Rule Based Dynamic Access Pt1 | Have the mission systems implemented rule-based dynamic access using user identity and other non-static attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | Have the mission systems implemented rule-based dynamic access using user identity and other attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | In Process | |
| 4 | 1.3 - Multi-Factor Authentication | 1.3.1 | Organizational MFA/IDP | Has the mission system implemented and IdP and MFA solution that is integrated with the enteprise PKI system? | Has the mission system implemented multi-factor authentication, supporting multiple DoD-approved hardware and mobile authenticators to accommodate a wide range of users, devices, partners, mission environments, scenarios, and security access levels?<br>Are the IdP and MFA solutions integrated with the enteprise PKI system? | Complete | |
| 5 | 1.4 - Privileged Access | 1.4.1 | Implement System and Migrate Privileged Users Pt1 | Have you removed of permanent administrator/elevated privileges, implemented a Privileged Account Management (PAM) solution and migrated privileged users to it? Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | Has the mission system removed permanent administrator/elevated privileges, implemented a Privileged Access Management (PAM) system, and migrated privileged users who require access to the PAM user list?<br><br>Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | N/A | |
| 6 | 1.4 - Prigileged Access | 1.4.2 | Implement System and Migrate Privileged Users Pt2 | Have all privileged activities been migrated to the PAM solution? Have unsupported or challenging applications/services been integrated with the PAM solution? Have all remaining applications that cannot be integrated been identified for decommissioning? Are the remaining non-integrated applications being managed in a risk based manner with compensating controls? | Have all privileged activities been migrated to the PAM solution? Have unsupported or challenging applications/services been integrated with the PAM solution?<br>Have all remaining applications that cannot be integrated been identified for decommissioning?<br>Are the remaining non-integrated applications being managed in a risk based manner with compensating controls? | Not Answered | |

Detailed activity information can be ungrouped

Pillar Results Aggregated

Notes collected on current or next steps or action

Pillar Worksheets collect assessment results on activities

Basic ZT Capability and related Target Activity information

Source: SSC/S6 ZT Self-Evaluation

# Core Self-Evaluation Framework Content

Detailed activity information ungrouped

**Pillar: USER**

For additional Capability and ZT Target Information use the + signs above to expand each section

| Responses | Totals | Average |
|---|---|---|
| Not Answered | 3 | 23.08% |
| Not Started | 3 | 23.08% |
| In Process | 3 | 23.08% |
| Complete | 2 | 15.38% |
| N/A | 2 | 15.38% |

| Number | DoD Zero Trust Capability | Capability Description | Capability Outcome | Impact to ZT | Associated Activities | ID# | Target Level Activity Name | Target Control ID and Activity | Responsible | Descriptions | Outcomes | End State | Predecessor(s) | Successor(s) | DOD Target Level Activities Supplemental Info | Clarifying Questions to Identify Activity Intent | Status (Dropdown) | | | Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.1 - User Inventory | Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted. | System owners have control/visibility and administrative rights/roll of all authorized and authenticated users on the network. | Users not on the authorized user list will be denied access by policy. | *Inventory User | 1.1.1 | Inventory User | 1.1.1 - Inventory User | Component | DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE: AMED, NSS, ARS) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity lifecycle management processes (i.e. joiner/mover/leaver/returner). If privileged users are clearly identified. | 1. Identified managed non-privileged users.<br>2. Identified managed privileged users.<br>3. Identified applications using their own user account management for non-administrative and administrative accounts.<br>4. Identify the authoritative source of identities. | Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the most up-to-date user data. | | Rule Based Dynamic Access Pt2 | Have the mission areas identified and inventoried regular and privileged users registered in the ICAM system and in local applications, systems, or services that may not yet be integrated with the ICAM system? | Have the mission areas inventoried and catalogued all users within the organization who have or require verified access to the mission system?<br>Have the standard and privileged accounts been identified? | Not Answered | | | |
| 2 | 1.2 - Conditional User Access | Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federated ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules. | Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments. | Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy. | * Implement App Based Permissions per Enterprise<br>* Rule Based Dynamic Access Pt1<br>* Rule Based Dynamic Access Pt2<br>* Enterprise Gov't roles and Permissions Pt1<br>* Enterprise Gov't roles and Permissions Pt2 | 1.2.1 | Implement App Based Permissions per Enterprise | 1.2.1 - Implement App Based Permissions per Enterprise | Enterprise and Component | The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process to accomplish Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation.<br>Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles. | 1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been vetted and approved through the ICAM governance processes.<br>2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e. attributes and entitlements), while maximizing the usage of self-service attributes and entitlements.<br>3. Components identity attributes associated with PAM activities within their environment.<br>4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once, available, or from other Components using standard profiles. | Authoritative attributes required to implement conditional user access into applications are available to support privileged access management. | | | Have the mission areas established and implemented a standard set of permissions and attributes for each app/resource using the unified enterprise ICAM solution as a requirement for subjects seeking access to the app/resource?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add/update authorization attributes? | Have the mission areas unified and integrated the ICAM solutions using federation where applicable?<br>Have the mission areas established and implemented a standard set of permissions and attributes for each app/resource - using the unified enterprise ICAM solution?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add/update authorization attributes? | Not Started | | | |
| 3 | 1.2 - Conditional User Access | Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federated ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules. | Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments. | Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy. | * Implement App Based Permissions per Enterprise<br>* Rule Based Dynamic Access Pt1<br>* Rule Based Dynamic Access Pt2<br>* Enterprise Gov't roles and Permissions Pt1<br>* Enterprise Gov't roles and Permissions Pt2 | 1.2.2 | Rule Based Dynamic Access Pt1 | 1.2.2 - Rule Based Dynamic Access Pt1 | Component | DoD Components utilize the rules from the "Periodic Authentication" activity to build roles enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-In-Time (JIT) access and Just-Enough-Administration (JEA) methods. | 1. Access to an application's/services' functions and/or data are limited to users with appropriate Attribute-Based Access Control (users, devices, environment etc.), allowing for granular and flexible control.<br>2. All possible applications use RTIDEA permissions for administrative users. | Periodic challenges occur when access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real-time. | Single Authentication; Inventory User | Rule Based Dynamic Access Pt2; AI-enabled Network Access | Have the mission systems implemented rule-based dynamic access using user identity and other non-static attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (RTIDEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | Have the mission systems implemented rule-based dynamic access using user identity and other attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (RTIDEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | In Process | | | |
| 4 | 1.3 - Multi-Factor Authentication | This capability initially focuses on developing an organization focused MFA provider and Identity Provider to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical precursor to this capability. Alternatively, it levels alternative and flexible MFA tokens can be used to provide access for standard and external users. | Do DO organizations require users and non-user entities to authenticate using at least two of the following three attributes; knowledge (something they know), possession (CAC/token), or something you are (inherence, e.g., iris/fingerprints), in order to access DAAS. | Users not presenting multiple forms of authentication will be denied access to DAAS systems and resources. | * Organizational MFA/IDP<br>* Alternative Flexible MFA Pt1<br>* Alternative Flexible MFA Pt2 | 1.3.1 | Organizational MFA/IDP | 1.3.1 - Organizational MFA/IDP | Component | DoD Components or Identity Provider (IdP) solution using approved credential or approved alternative Multi-Factor Authentication (MFA). The IdP and MFA solution may be combined in a single application or separated as needed assuming automated integration is supported by both solutions. Both IdP and MFA support integration with the Enterprise PKI capability as well as enabling key pairs to be signed by the trusted root certificate authorities. Authentication for mission/task-critical applications and services authentication is MFA-Enabled and leverages the related authentication mechanisms to manage users and groups. | 1. Component is using IdP with MFA for critical applications/services.<br>2. Components have implemented an Identity Provider (IdP) that enables DoD PKI/Multi-Factor Authentication (e.g. CAC, DPIV, DoD Issued PIV-I, NIPS 201 Compliant softcerts).<br>3. DO Enterprise has approved organizational PKI for critical services (ECA, FPKI, Category I/II/III PKI, etc.).<br>4. Utilize approved Alternative Hardware Tokens as needed - (USB Security Key and/or OTP device (e.g. Yubiley NPS for smartcard, RSD2, RSD-U2F, OTP, RSA SecurID for OTP, etc.).<br>5. For access to low-risk resources (e.g., FR, publicly released information), utilize alternative two-step, two-factor authentication using software authenticators (i.e., Mobile Connect, Yubico, Okta Verify, etc.). | Critical applications are identified and use MFA in alignment with a federated IdP solution. | | | Implement System and Migrate Privileged Users Pt2 | Have the mission system implemented and IdP and MFA solution that is integrated with the enterprise PKI system? | Has the mission system implemented multi-factor authentication, supporting multiple DoD-approved hardware and mobile authenticators to accommodate a wide range of users, devices, partners, mission environments, scenarios, and security access levels?<br>Are the IdP and MFA solutions integrated with the enterprise PKI system? | Complete | | | |
| 5 | 1.4 - Privileged Access | The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection. | Do DO organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, RTIDEA with PAWS) across their IT environments. | Critical assets and applications secured, controlled, monitored and managed through limits on admin access. | * Implement System and Migrate Privileged Users Pt1<br>* Implement System and Migrate Privileged Users Pt2<br>* Real time Approvals & RTIDEA Analytics Pt1<br>* Real time Approvals & RTIDEA Analytics Pt2 | 1.4.1 | Implement System and Migrate Privileged Users Pt1 | 1.4.1 - Implement System and Migrate Privileged Users Pt1 | Component | DoD Components procure and implement a Privileged Access Management (PAM) solution to support all critical privileged use cases. Application/Service integration points are identified to determine status of support for the PAM solution. Applications/Services that are integrated with the PAM solution are transitioned to using the solution versus static and direct privileged permissions. | 1. Privilege Access Management (PAM) tooling is implemented.<br>2. Applications and devices that support and do not support PAM tools are identified.<br>3. Applications that support PAM, now use PAM for controlling emergency/built-in accounts. | Components implement a PAM tool with a clear transition plan that identifies the applications and decides what applications require a PAM tool. | | Implement System and Migrate Privileged Users Pt2 | Have you removed of permanent administrator/elevated privileges, implemented a Privileged Account Management (PAM) solution and migrated privileged users to it? Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | Has the mission system removed permanent administrator/elevated privileges, implemented a Privileged Access Management (PAM) system, and migrated privileged users who require access to the PAM user list?<br>Have applications that are challenging to integrate with the PAM solution been identified? Have you transitioned applications and services that are can be easily integrated to the PAM solution? | N/A | | | |
| 6 | 1.4 - Pngileged Access | The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection. | Do DO organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, RTIDEA with PAWS) across their IT environments. | Critical assets and applications secured, controlled, monitored and managed through limits on admin access. | * Implement System and Migrate Privileged Users Pt1<br>* Implement System and Migrate Privileged Users Pt2<br>* Real time Approvals & RTIDEA Analytics Pt1<br>* Real time Approvals & RTIDEA Analytics Pt2 | 1.4.2 | Implement System and Migrate Privileged Users Pt2 | 1.4.2 - Implement System and Migrate Privileged Users Pt2 | Component | DoD Components utilize the inventory of supported and unsupported Application/Services for integration with the Privileged Access Management (PAM) solution to extend integrations. PAM is integrated with the more challenging Applications/Services to maximize PAM solution coverage. Exceptions are managed in a risk-based methodical approach with the goal of migration of and/or decommissioning Applications/Services that do not support the PAM solution. | 1. Privileged activities are migrated to PAM and access is fully managed. | Ensure secure and controlled access to privileged accounts and resources through fully implemented PAM solution, mitigating the risk of unauthorized access and potential cyberthreats. | Implement System and Migrate Privileged Users Pt1 | Real time Approvals & RTIDEA Analytics Pt1 | Have all privileged activities been migrated to the PAM solution? Have unsupported or challenging applications/services been integrated with the PAM solution? Have all remaining applications that cannot be migrated been identified for decommissioning? Are the remaining non-integrated applications being managed in a risk based manner with compensating controls? | Have all privileged activities been migrated to the PAM solution? Have unsupported or challenging applications/services been integrated with the PAM solution? Have all remaining applications that cannot be migrated been identified for decommissioning? Are the remaining non-integrated applications being managed in a risk based manner with compensating controls? | Not Answered | | | |
| 7 | 1.5 - Identity Federation & User Credentialing | The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDP solution. Once completed the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or identity federation. | Do DO organizations manually issue, manage, and revoke credentials bound to DoD person, device, and NPE identities. Identity information is developed and shared across entities and trust domains providing "single sign-on" convenience and efficiencies to identified (authenticated and authorized) users and devices. | Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies. | * Organizational Identity Life-Cycle Management<br>* Enterprise Identity Life-Cycle Management Pt1<br>* Enterprise Identity Life-Cycle Management Pt2<br>* Enterprise Identity Life-Cycle Management Pt3 | 1.5.1 | Organizational Identity Life-Cycle Management | 1.5.1 - Organizational Identity Life-Cycle Management | Component | DoD Components establish a process for life cycle management of users both privileged and non-privileged. Utilizing an approved Identity Provider (IdP) the process is implemented and followed by the maximum number of users. Users lacking a portion of the standard process are approved through risk-based exceptions to be evaluated regularly for decommission. | 1. Standardized account life cycle process. | Establishes a comprehensive and efficient process that ensures the accurate and secure management of user identities throughout their entire life cycle within the Components environment. | | Enterprise Identity Life-Cycle Management Pt2 | Has a process been established for lifecycle management for the maximum amount of users leveraging the enterprise ICAM and IdP? Is there a process that identifies and keeps track of users who may fall outside this process for decommission? Users who fall outside this process must be approved through risk-based exceptions. | Has a process been established for lifecycle management for the maximum possible number of users leveraging the enterprise ICAM and IdP? Is there a process that identifies and keeps track of users who may fall outside this process for decommission? Users who fall outside this process must be approved through risk-based exceptions.<br>Have the users who fall outside this process been approved through risk-based exceptions? | Not Started | | | |
| 8 | 1.5 - Identity Federation & User Credentialing | The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDP solution. Once completed the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or identity federation. | Do DO organizations manually issue, manage, and revoke credentials bound to DoD person, device, and NPE identities. Identity information is developed and shared across entities and trust domains providing "single sign-on" convenience and efficiencies to identified (authenticated and authorized) users and devices. | Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies. | * Organizational Identity Life-Cycle Management<br>* Enterprise Identity Life-Cycle Management Pt1<br>* Enterprise Identity Life-Cycle Management Pt2<br>* Enterprise Identity Life-Cycle Management Pt3 | 1.5.2 | Enterprise Identity Life-Cycle Management Pt 1 | 1.5.2 - Enterprise Identity Life-Cycle Management Pt 1 | Enterprise and Component | Specified policies and supporting process are followed by DoD Components. DoD Components implement Identity Life-Cycle Management process for the maximum number of identities, attributes, groups, credentials, and permissions. Exceptions to the policy are managed in a risk-based methodical approach. | 1. Automated identity life cycle processes.<br>2. Integrated with Enterprise ICAM processes and tools. | Implementation of consistent and well-defined processes and controls for managing the maximum number of identities in the life cycle. | Organizational Identity Life-Cycle Management | Enterprise Identity Life Cycle Management Pt2 | Have identity Lifecycle Processes, policy, and standards been developed and finalized? Are the enterprise ICAM and IdP being leveraged to implement the Enterprise Lifecycle Management process for the maximum number of identities, groups, and permissions? Are exceptions to the policy are managed in a risk based methodical approach? | Have identity Lifecycle Processes, policy, and standards been developed and finalized? Are the enterprise ICAM and IdP being leveraged to implement the Enterprise Lifecycle Management process for the maximum number of identities, groups, and permissions? Are exceptions to the policy are managed in a risk based methodical approach? | In Process | | | |
| 9 | 1.6 - Behavioral, Contextual ID, & Biometrics | Leveraging this Enterprise IdP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once complete this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally UEBA are integrated with the PAM and RTIDEA systems to better detect anomalous and | Do DO organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls. | Behavioral, contextual, and biometric telemetry enhances MFA with | * Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling<br>* User Activity Monitoring Pt1<br>* User Activity Monitoring Pt2 | 1.6.1 | Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling | 1.6.1 - Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling | Component | DoD Components procure and implement User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions. Initial integration point with Enterprise IdP is completed, enabling future usage in decision making. | 1. UEBA and UAM functionality is correlated with the Master User Record and integrated with Enterprise IdP. | Establish a comprehensive and continuously adaptive security solution that leverages behavior analytics, detects anomalies, and protects against unauthorized access. | | Establish User Baseline Behavior; User/Device Baselines Alternative Flexible MFA Pt2 | Has enterprise IdP integration with User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions been completed? | Has enterprise IdP integration with User & Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) solutions been completed? | Complete | | | |
| 10 | 1.7 - Least Privileged Access | Do DO organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. Do Application Owners identify the necessary roles and required attributes for standard and privileged user access. Privileged access for all Do DO organization DAAS is audited and removed when unneeded. | Do DO organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. | Users on the network initially have access to the DAAS for which they are authorized and authenticated over a specific timeframe. | * Deny User by Default Policy | 1.7.1 | Deny User by Default Policy | 1.7.1 - Deny User by Default Policy | Component | Do DO Components audit user and group usage for permissions and revoke permissions when appropriate. This activity includes the revocation and/or decommission of excess permissions and access for application/service-based identities and groups. Where possible, static privileged users are decommissioned or permissions are reduced, preparing for future role/dynamic based access. The implemented audit and governance functions are automated where possible. | 1. Applications updated to deny by default to functions/data requiring specific roles/attributes for access.<br>2. Reduced default permission levels are implemented.<br>3. Applications/services privileged users have been reviewed and audited, and unnecessary access has been removed.<br>4. Applications' identity functions and data requiring specific roles/attributes for access.<br>5. Audit functions and governance processes are implemented and automated when possible to update user authentication and authorization. | Users must be authorized and authenticated to access data, applications, assets, and services. Audit and access validation occurs consistently. | | | Is there a process to audit internal user and group permissions and to revoke or remove excess permissions? Have static privileged user accounts been decommissioned or have their permissions been reduced? | Is there a process to audit internal user and group permissions and to revoke or remove excess permissions? Have static privileged user accounts been decommissioned or have their permissions been reduced? | N/A | | | |
| 11 | 1.8 - Continuous Authentication | The DO organizations and overall enterprise will methodically move towards continuous attributes based authentication. Initially the capability focuses on standardizing legacy single authentication to a organizationally approved IDP with users and groups. The second stages adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and | Do DO organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA. | Users not continuously presenting multiple forms of authentication will be denied access to DAAS systems and resources. | * Single Authentication<br>* Periodic Authentication<br>* Continuous Authentication Pt1<br>* Continuous Authentication Pt2 | 1.8.1 | Single Authentication | 1.8.1 - Single Authentication | Component | Do DO Components authenticate users and NPE's at least once per session (e.g., login) using CAC and other Do DO approved methods. Users being authenticated are managed to the parallel activity "Organizational MFA/IDP" with the Component Identity Provider (IdP). Components do not use application/service-based identities and groups. | 1. Authentication implemented at least once per session. | Component applications apply single authentication to the specified standard. | | Rule Based Dynamic Access Pt1 Resource Authorization Pt1; SDC Resource Authorization Pt2 | Have mission systems implemented at least a single authentication per session leveraging the enterprise ICAM solution? | Have mission systems implemented at least a single authentication per session for users with the enterprise ICAM solution? (Are users or NPEs authenticated at least once per session?) | Not Answered | | | |
| 12 | 1.8 - Continuous Authentication | The DO organizations and overall enterprise will methodically move towards continuous attributes based authentication. Initially the capability focuses on standardizing legacy single authentication to a organizationally approved IDP with users and groups. The second stages adds in based rule based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and | Do DO organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA. | Users not continuously presenting multiple forms of authentication will be denied access to DAAS systems and resources. | * Single Authentication<br>* Periodic Authentication<br>* Continuous Authentication Pt1<br>* Continuous Authentication Pt2 | 1.8.2 | Periodic Authentication | 1.8.2 - Periodic Authentication | Component | Do DO Components enable periodic authentication for applications and services. Traditionally, these are based on a duration and/or duration timeout, however, other period-based analytics can be used to enforce re-authentication of user sessions. | 1. Authentication implemented multiple times per session based on security attributes and criticality of the data, user, application, system, and source user location. | Authentication occurs per the requirement and standard. | Single Authentication | Continuous Authentication Pt1; AI-enabled Network Access | Has the mission system implemented continuous authentication and auditing of ICAM events? Are subjects requesting access asked to re-authenticate at intervals? | Has the mission system implemented continuous authentication, monitoring and auditing of ICAM events? | Not Started | | | |
| 13 | 1.9 - Integrated ICAM Platform | DO Organizations and overall enterprise employ enterprise-level identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized | Do DO organizations employ enterprise-level identity management systems to track user and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, identity governance and administration tools, and an access management tool. | Identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms. | * Enterprise PKI/IDP Pt1<br>* Enterprise PKI/IDP Pt2<br>* Enterprise PKI/IDP Pt3 | 1.9.1 | Enterprise PKI/IDP Pt1 | 1.9.1 - Enterprise PKI/IDP Pt1 | Enterprise and Component | The DoD Enterprise works with Components to implement Enterprise Public Key Infrastructure (PKI) solutions in a centralized and/or federated fashion. The Enterprise PKI solution utilizes a single or set of Enterprise-level Root Certificate Authorities (CA) that can then be issued by components to build Intermediate CA. Components PKI Certificated Authorities are integrated with the Enterprise PKI. An Enterprise Identity Provider (IdP) platform is implemented. The IdP solution may either be a single solution or federated set of Component IdPs with standard level of access across Components and standardized set of attributes. Components IdPs are integrated with the Enterprise IdP. | 1. Enterprise PE & NPE CONOPS, taxonomy, and naming standards are developed.<br>2. Components Certificate Authorities (CA) are integrated with the DoD PKI Hierarchy.<br>3. Enterprise-level requirements are implemented, including mandated user attributes for available and verified Enterprise Identity Provider (IdP) Platform.<br>4. Enterprise wide IdP platform is implemented through a single solution or integration of multiple solutions. | All PEs and NPEs are issued available and verified digital identity that can be tracked at the Enterprise level using the strongest authentication available. | | Enterprise PKI/IDP Pt2 | Is the enterprise IdP integrated with the enterprise PKI solution? (The enterprise PKI solution can be a multi-tier architecture) (The enterprise IdP could be integrated with other organizational IdPs using federation) | Is the enterprise IdP (including a federated set of IdPs) integrated with the enterprise PKI solution? (The enterprise PKI solution can be a multi-tier architecture) | In Process | | | |

Source: SSC/S6 ZT Self-Evaluation

# Ungrouped Capability/Activity Details

## BASIC ZT CAPABILITY AND TARGET LEVEL ACTIVITY INFORMATION

- Number (Worksheet Key)
- DoD Zero Trust Capability*
- Basic ZT Capaiblity Information*
  - Capability Description*
  - Capability Outcome*
  - Impact to ZT*
  - Associated Activities*
- Target Activity Information *
  - Target Activity ID#*
  - Target Level Activity Name*
  - Control ID and Activity*
  - Responsibility*
  - Descriptions*
  - Outcomes*
  - End State*
  - Predecessor(s)*
  - Successor(s)*
- DOD Target Level Activities Supplemental Info
- Clarifying Questions to Identify Activity Intent
- Status (*Dropdown Selection*)
- Notes (*Free Text*)

Source of ZT Details: * DoD Zero Trust Execution Roadmap, 22 Jan 2025

# Example - User Pillar 1.1

## S6 ZT Self-Evaluation – User Pillar 1.1

| Number | DoD Zero Trust Capability | Capability Description | Capability Outcome | Impact to ZT | Associated Activities | ID# | Target Level Activity Name | Target Control ID and Activity | Responsibility | Descriptions | Outcomes | End State | Predecessor(s) | Successor(s) | DOD Target Level Activities Supplemental Info | Clarifying Questions to Identify Activity Intent |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.1 - User Inventory | Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted. | System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network. | Users not on the authorized user list will be denied access by policy. | * Inventory User | 1.1.1 | Inventory User | 1.1.1 - Inventory User | Component | DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified. | 1. Identified managed non-privileged users.<br>2. Identified managed privileged users.<br>3. Identified applications using their own user account management for non-administrative and administrative accounts.<br>4. Identify the authoritative source of identities. | Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to- date user data. | | Rule Based Dynamic Access Pt1 | Have the mission areas identified and inventoried regular and privileged users registered in the ICAM system and in local applications, systems, or services that may not yet be integrated with the ICAM system? | Have the mission areas inventoried and cataloged all users within the organization who have or require verified access to the mission system?<br>Have the standard and privileged accounts been identified? |

Source: SSC/S6 ZT Self-Evaluation

## Basic ZT Capability– User Pillar 1.1

| ID # | Capability | Pillar | Capability Description | Capability Outcome | Impact to ZT | Associated Activities |
|---|---|---|---|---|---|---|
| 1.1 | User Inventory | 1 - User | Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted. | System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network. | Users not on the authorized user list will be denied access by policy. | * Inventory User |

Source: * DoD Zero Trust Execution Roadmap, 22 Jan 2025

1:1 mapping of Basic Capabilities to Target Activities

## Target Activity - User Pillar 1.1.1

| ID# | Activity Name | Pillar | Responsibility | Activity Type | Duration | Descriptions | Outcomes | End State | Predecessor(s) | Successor(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.1.1 | Inventory User | User | Component | Target Level ZT | 25.9 | DoD Components utilize Enterprise authoritative source of (PE/NPE) identity (PE - AMID, NIS, AFID) and/or establish or augment with local authoritative source. Identity management can be done manually if needed, preparing for automated approach in later stages. Identity source is connected to identity life cycle management processes (i.e. joiner/mover/leaver/returner). IT privileged users are clearly identified. | 1. Identified managed non-privileged users.<br>2. Identified managed privileged users.<br>3. Identified applications using their own user account management for non-administrative and administrative accounts.<br>4. Identify the authoritative source of identities. | Accurately determine and keep track of users who have both the authorization and authentication to access critical systems or resources. This involves regularly reviewing, communicating, and carefully examining the sources of information that provide the true and up-to-date user data. | | Rule Based Dynamic Access Pt1 |

Source: * DoD Zero Trust Execution Roadmap, 22 Jan 2025

# Example - User Pillar 1.2

## S6 ZT Self-Evaluation – User Pillar 1.2

| Number | DoD Zero Trust Capability | Capability Description | Capability Outcome | Impact to ZT | Associated Activities | ID# | Target Level Activity Name | Target Control ID and Activity | Responsibility | Descriptions | Outcomes | End State | Predecessor(s) | Successor(s) | DOD Target Level Activities Supplemental Info | Clarifying Questions to Identify Activity Intent |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 1.2 - Conditional User Access | *Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.* | *Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments.* | *Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy.* | * Implement App Based Permissions per Enterprise<br>* Rule Based Dynamic Access Pt1<br>* Rule Based Dynamic Access Pt2<br>* Enterprise Gov't roles and Permissions Pt1<br>* Enterprise Gov't roles and Permissions Pt2 | 1.2.1 | Implement App Based Permissions per Enterprise | 1.2.1 - Implement App Based Permissions per Enterprise | Enterprise and Component | *The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles.* | *1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been vetted and approved through the ICAM governance processes.<br>2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e. attributes and entitlements), while maximizing the usage of self- service attributes and entitlements.<br>3. Components identify attributes associated with PAM activities within their environment.<br>4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once. available, or from other Components using standard profiles.* | *Authoritative attributes requiired to implement conditional user access into applications are available to support privileged access management.* | | | Have the mission systems established and implemented a standard set of permissions and attributes for each app/resource using the unified enterprise ICAM solution as requirement for subjects seeking access to the app/resource?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add authorization attributes? | Have the mission areas unified and integrated the ICAM solutions using federation where applicable?<br>Have the mission areas established and implemented a standard set of permissions and attributes for each app/resource - using the unified enterprise ICAM solution?<br>Are all privileged account management processes and activities integrated with, or managed using the enterprise ICAM solution?<br>Is a self-service feature included that allows designated application owners to register or add/specify authorization attributes? |
| 3 | 1.2 - Conditional User Access | *Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.* | *Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments.* | *Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy.* | * Implement App Based Permissions per Enterprise<br>* Rule Based Dynamic Access Pt1<br>* Rule Based Dynamic Access Pt2<br>* Enterprise Gov't roles and Permissions Pt1<br>* Enterprise Gov't roles and Permissions Pt2 | 1.2.2 | Rule Based Dynamic Access Pt1 | 1.2.2 - Rule Based Dynamic Access Pt1 | Component | *DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just-Enough- Administration (JEA) methods.* | *1. Access to an applications'/services' functions and/or data are limited to users with appropriate Attribute-Based Access Control (users, devices, environment etc.), allowing for granular and flexible control.<br>2. All possible applications use JIT/JEA permissions for administrative users.* | *Periodic challenges occur where access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real-time.* | *Single Authentication; Inventory User* | *Rule Based Dynamic Access Pt2; AI-enabled Network Access* | Have the mission systems implemented rule-based dynamic access using user identity and other non-static attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? | Have the mission systems implemented rule-based dynamic access using user identity and other non-static attributes, such as device posture, location, time of day, and data sensitivity?<br>Are the mission systems leveraging data sensitivity attribute based on tagged and labeled data to make access and authorization decisions?<br>Are high risk accounts using the privileged account management solution to request on-demand access (JIT/JEA) to sensitive systems and applications?<br>Is periodic authentication implemented forcing re-authentication of users? |

Source: SSC/S6 ZT Self-Evaluation

| ID # | Capability | Pillar | Capability Description | Capability Outcome | Impact to ZT | Associated Activities |
|---|---|---|---|---|---|---|
| 1.2 | Conditional User Access | 1 - User | Through maturity levels Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role based access controls across a federate ICAM, expands to be application focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules. | Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine grained access control to include the use of user risk assessments. | Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy. | * Implement App Based Permissions per Enterprise<br>* Rule Based Dynamic Access Pt1<br>* Rule Based Dynamic Access Pt2<br>* Enterprise Gov't roles and Permissions Pt1<br>* Enterprise Gov't roles and Permissions Pt2 |

Source: * DoD Zero Trust Execution Roadmap, 22 Jan 2025

| ID# | Activity Name | Pillar | Responsibility | Activity Type | Duration | Descriptions | Outcomes | End State | Predecessor(s) | Successor(s) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.2.1 | Implement App Based Permissions per Enterprise | User | Enterprise and Component | Target Level ZT | 17.7 | The DoD ICAM governance establishes a set of user attributes for authentication and authorization. These are integrated with the "Enterprise Identity Life-Cycle Management Pt1" activity process for a complete Enterprise standard. The Enterprise Identity, Credential and Access Management (ICAM) solution are enabled for adding/updating attributes within the solution to better support identity federation. Remaining Privileged Access Management (PAM) activities are approved and tailored as specified by roles. | 1. Enterprise roles/attributes needed for user authorization to application functions and/or data have been-vetted and approved through the ICAM governance processes.<br>2. Approved Component ICAM implementations will maintain and make available authoritative information about their personnel (i.e. attributes and entitlements), while maximizing the usage of self-service attributes and entitlements.<br>3. Components identify attributes associated with PAM activities within their environment.<br>4. Component ICAM implementation obtain authoritative information about personnel (i.e. attributes, and entitlements) from a central attribute source once. available, or from other Components using standard profiles. | Authoritative attributes requiired to implement conditional user access into applications are available to support privileged access management. | | |
| 1.2.2 | Rule Based Dynamic Access Pt1 | User | Component | Target Level ZT | 22.1 | DoD Components utilize the rules from the "Periodic Authentication" activity to build rules enabling and disabling privileges dynamically. IT Privileged user accounts utilize the PAM solution to move to dynamic privileged access using Just-in-Time (JIT) access and Just-Enough-Administration (JEA) methods. | 1. Access to an applications'/services' functions and/or data are limited to users with appropriate Attribute-Based Access Control (users, devices, environment etc.), allowing for granular and flexible control.<br>2. All possible applications use JIT/JEA permissions for | Periodic challenges occur where access is affected if challenge is failed within accepted response parameters. Access is always predicated on authentication and authorization with activity happening (decisions made) in real-time. | Single Authentication; Inventory User | Rule Based Dynamic Access Pt2; AI-enabled Network Access |

1:many mapping of Basic Capabilities to Target Activities



Source: * DoD Zero Trust Execution Roadmap, 22 Jan 2025

# Assessment End Result

## Pillar: USER

For additional Capability and ZT Target Information use the '+' signs avove to expand each section

| Responses | Totals | Average |
|---|---|---|
| Not Answered | 1 | 7.69% |
| Not Started | 3 | 23.08% |
| In Process | 3 | 23.08% |
| Complete | 3 | 23.08% |
| N/A | 3 | 23.08% |

N/A and No Responses require a comment

| Number | DoD Zero Trust Capability | ID# | Target Level Activity Name | Status (Dropdown) | | | Notes |
|---|---|---|---|---|---|---|---|
| 1 | 1.1 - User Inventory | 1.1.1 | Inventory User | Not Answered | | | |
| 2 | 1.2 - Conditional User Access | 1.2.1 | Implement App Based Permissions per Enterprise | Not Started | | | |
| 3 | 1.2 - Conditional User Access | 1.2.2 | Rule Based Dynamic Access Pt1 | In Process | | | |
| 4 | 1.3 - Multi-Factor Authentication | 1.3.1 | Organizational MFA/IDP | Complete | | | |
| 5 | 1.4 - Privileged Access | 1.4.1 | Implement System and Migrate Privileged Users Pt1 | N/A | | | |
| 6 | 1.4 - Prigileged Access | 1.4.2 | Implement System and Migrate Privileged Users Pt2 | Not Started | | | |
| 7 | 1.5 - Identify Federation & User Credentialing | 1.5.1 | Organizational Identity Life- Cycle Management | In Process | | | |
| 8 | 1.5 - Identify Federation & User Credentialing | 1.5.2 | Enterprise Identity Life-Cycle Management Pt 1 | Complete | | | |
| 9 | 1.6 - Behavioral, Contextual ID, & Biometrics | 1.6.1 | Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling | N/A | | | |
| 10 | 1.7 - Least Privileged Access | 1.7.1 | Deny User by Default Policy | Not Started | | | |
| 11 | 1.8 - Continuous Authentication | 1.8.1 | Single Authentication | In Process | | | |
| 12 | 1.8 - Continuous Authentication | 1.8.2 | Periodic Authentication | Complete | | | |
| 13 | 1.9 - Integrated ICAM Platform | 1.9.1 | Enterprise PKI/IDP Pt1 | N/A | | | |

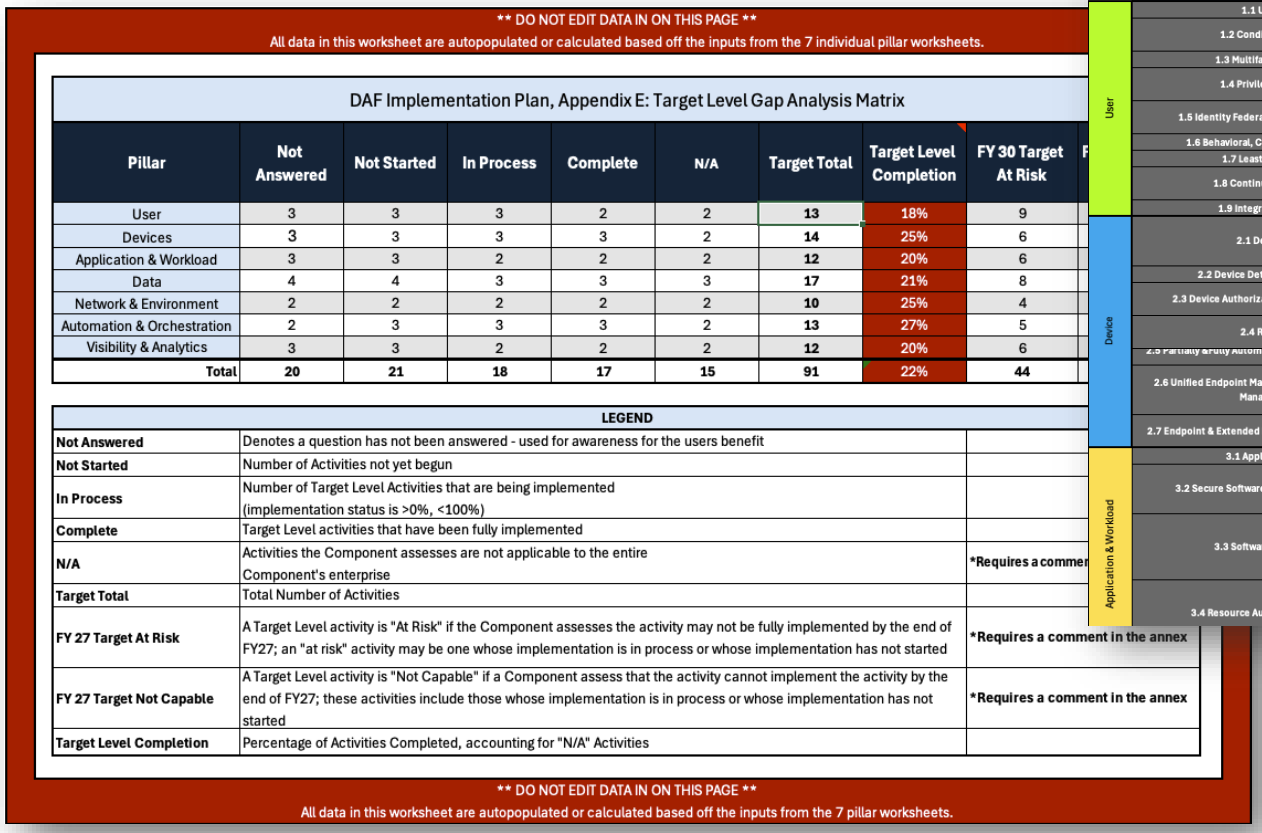


Source: SSC/S6 ZT Self-Evaluation

# Leveraging Assessment Data

Once Collected, evaluation data informs:

- Target Gap Analysis Worksheet, and
- Tab 4. DoD ZT Capabilities



** DO NOT EDIT DATA IN ON THIS PAGE **

All data in this worksheet are autopopulated or calculated based off the inputs from the 7 individual pillar worksheets.

DAF Implementation Plan, Appendix E: Target Level Gap Analysis Matrix

| Pillar | Not Answered | Not Started | In Process | Complete | N/A | Target Total | Target Level Completion | FY 30 Target At Risk |
|---|---|---|---|---|---|---|---|---|
| User | 3 | 3 | 3 | 2 | 2 | 13 | 18% | 9 |
| Devices | 3 | 3 | 3 | 3 | 2 | 14 | 25% | 6 |
| Application & Workload | 3 | 3 | 2 | 2 | 2 | 12 | 20% | 6 |
| Data | 4 | 4 | 3 | 3 | 3 | 17 | 21% | 8 |
| Network & Environment | 2 | 2 | 2 | 2 | 2 | 10 | 25% | 4 |
| Automation & Orchestration | 2 | 3 | 3 | 3 | 2 | 13 | 27% | 5 |
| Visibility & Analytics | 3 | 3 | 2 | 2 | 2 | 12 | 20% | 6 |
| Total | 20 | 21 | 18 | 17 | 15 | 91 | 22% | 44 |

| LEGEND | | |
|---|---|---|
| Not Answered | Denotes a question has not been answered - used for awareness for the users benefit | |
| Not Started | Number of Activities not yet begun | |
| In Process | Number of Target Level Activities that are being implemented (implementation status is >0%, <100%) | |
| Complete | Target Level activities that have been fully implemented | |
| N/A | Activities the Component assesses are not applicable to the entire Component's enterprise | *Requires a commer |
| Target Total | Total Number of Activities | |
| FY 27 Target At Risk | A Target Level activity is "At Risk" if the Component assesses the activity may not be fully implemented by the end of FY27; an "at risk" activity may be one whose implementation is in process or whose implementation has not started | *Requires a comment in the annex |
| FY 27 Target Not Capable | A Target Level activity is "Not Capable" if a Component assess that the activity cannot implement the activity by the end of FY27; these activities include those whose implementation is in process or whose implementation has not started | *Requires a comment in the annex |
| Target Level Completion | Percentage of Activities Completed, accounting for "N/A" Activities | |

** DO NOT EDIT DATA IN ON THIS PAGE **

All data in this worksheet are autopopulated or calculated based off the inputs from the 7 individual pillar worksheets.

Select the '+' sign above to expand the group and show results form the 7-pillar assessment

DoD ZT Capabilities

System Name: []

| | DoD ZT Capability | Implementation Status | Expected Implementation Timeline | Leveraging Enterprise Implementation Solution (Yes/No) | Enterprise Implementation Tool or Solution | Additional Enterprise Implementation Tool or Solution | Implementation Approach | Additional Notes |
|---|---|---|---|---|---|---|---|---|
| User | 1.1 User Inventory | | | | | | | |
| | 1.2 Conditional User Access | | | | | | | |
| | 1.3 Multifactor Authentication | | | | | | | |
| | 1.4 Privileged Access Mgmt. | | | | | | | |
| | 1.5 Identity Federation and User Credentialing | | | | | | | |
| | 1.6 Behavioral, Contextual ID, & Biometrics | | | | | | | |
| | 1.7 Least Privileged Access | | | | | | | |
| | 1.8 Continuous Authentication | | | | | | | |
| | 1.9 Integrated ICAM Platform | | | | | | | |
| Device | 2.1 Device Inventory | | | | | | | |
| | 2.2 Device Detection and Compliance | | | | | | | |
| | 2.3 Device Authorization w/ Real Time Inspection | | | | | | | |
| | 2.4 Remote Access | | | | | | | |
| | 2.5 Partially & Fully Automated Asset, Vulnerability and Patch | | | | | | | |
| | 2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM) | | | | | | | |
| | 2.7 Endpoint & Extended Detection & Response (EDR & XDR) | | | | | | | |
| Application & Workload | 3.1 Application Inventory | | | | | | | |
| | 3.2 Secure Software Development & Integration | | | | | | | |
| | 3.3 Software Risk Management | | | | | | | |
| | 3.4 Resource Authorization & Integration | | | | | | | |

Not Started
Dependent on Another DAF ZT Capability
In Progress
Delayed
Complete
Does Not Apply
Enterprise Solution Consideration



Source: SSC/S6 ZT Self-Evaluation

# Target Level Gap Analysis

Format extracted from implementation plan; single dashboard to track assessment across pillars.

** DO NOT EDIT DATA IN ON THIS PAGE **

All data in this worksheet are autopopulated or calculated based off the inputs from the 7 individual pillar worksheets.

**DAF Implementation Plan, Appendix E: Target Level Gap Analysis Matrix**

| Pillar | Not Answered | Not Started | In Process | Complete | N/A | Target Total | Target Level Completion | FY 30 Target At Risk | FY30 Target Not Capable |
|---|---|---|---|---|---|---|---|---|---|
| User | 3 | 3 | 3 | 2 | 2 | **13** | 18% | 9 | 2 |
| Devices | 3 | 3 | 3 | 3 | 2 | **14** | 25% | 6 | 2 |
| Application & Workload | 3 | 3 | 2 | 2 | 2 | **12** | 20% | 6 | 2 |
| Data | 4 | 4 | 3 | 3 | 3 | **17** | 21% | 8 | 3 |
| Network & Environment | 2 | 2 | 2 | 2 | 2 | **10** | 25% | 4 | 2 |
| Automation & Orchestration | 2 | 3 | 3 | 3 | 2 | **13** | 27% | 5 | 2 |
| Visibility & Analytics | 3 | 3 | 2 | 2 | 2 | **12** | 20% | 6 | 2 |
| **Total** | **20** | **21** | **18** | **17** | **15** | **91** | 22% | **44** | **15** |

| LEGEND | | |
|---|---|---|
| **Not Answered** | Denotes a question has not been answered - used for awareness for the users benefit | |
| **Not Started** | Number of Activities not yet begun | |
| **In Process** | Number of Target Level Activities that are being implemented (implementation status is >0%, <100%) | |
| **Complete** | Target Level activities that have been fully implemented | |
| **N/A** | Activities the Component assesses are not applicable to the entire Component's enterprise | ***Requires a comment in the annex** |
| **Target Total** | Total Number of Activities | |
| **FY 27 Target At Risk** | A Target Level activity is "At Risk" if the Component assesses the activity may not be fully implemented by the end of FY27; an "at risk" activity may be one whose implementation is in process or whose implementation has not started | ***Requires a comment in the annex** |
| **FY 27 Target Not Capable** | A Target Level activity is "Not Capable" if a Component assess that the activity cannot implement the activity by the end of FY27; these activities include those whose implementation is in process or whose implementation has not started | ***Requires a comment in the annex** |
| **Target Level Completion** | Percentage of Activities Completed, accounting for "N/A" Activities | |

** DO NOT EDIT DATA IN ON THIS PAGE **

All data in this worksheet are autopopulated or calculated based off the inputs from the 7 pillar worksheets.

Source: SSC/S6 ZT Self-Evaluation

# Template - DOD ZT Capabilities Worksheet

| DoD ZT Capabilities | | | | | | | |
|---|---|---|---|---|---|---|---|
| System Name: [] | | | | | | | |
| DoD ZT Capability | Implementation Status | Expected Implementation Timeline | Leveraging Enterprise Implementation Solution (Yes/No) | Enterprise Implementation Tool or Solution | Additional Enterprise Implementation Tool or Solution | Implementation Approach | Additional Notes |
| 1.1 User Inventory | | | | | | | |
| 1.2 Conditional User Access | | | | | | | |
| 1.3 Multifactor Authentication | | | | | | | |
| 1.4 Privileged Access Mgmt. | | | | | | | |
| 1.5 Identity Federation and User Credentialing | | | | | | | |
| 1.6 Behavioral, Contextual ID, & Biometrics | | | | | | | |
| 1.7 Least Privileged Access | | | | | | | |
| 1.8 Continuous Authentication | | | | | | | |
| 1.9 Integrated ICAM Platform | | | | | | | |

Not Started
Dependent on Another DAF ZT Capability
In Progress
Delayed
Complete
Does Not Apply
Enterprise Solution Consideration



Source: SSC/S6 ZT Self-Evaluation

# Modified Template – DOD ZT Capabilities

Assessment details available by ungrouping

Select the '+' sign above to expand the group and show results form the 7-pillar assessment

| | DoD ZT Capability | Implementation Status | Expected Implementation Timeline | Leveraging Enterprise Implementation Solution (Yes/No) | Enterprise Implementation Tool or Solution | Additional Enterprise Implementation Tool or Solution | Implementation Approach | Additional Notes |
|---|---|---|---|---|---|---|---|---|
| | **DoD ZT Capabilities** | | | | | | | |
| | **System Name: []** | | | | | | | |
| User | 1.1 User Inventory | In Progress | N/A | No | ICAM ID Provider | ICAM ID Governance | | |
| User | 1.2 Conditional User Access | | | | | | | |
| User | 1.3 Multifactor Authentication | | | | | | | |
| User | 1.4 Privileged Access Mgmt. | | | | | | | |
| User | 1.5 Identity Federation and User Credentialing | | | | | | | |
| User | 1.6 Behavioral, Contextual ID, & Biometrics | | | | | | | |
| User | 1.7 Least Privileged Access | | | | | | | |
| User | 1.8 Continuous Authentication | | | | | | | |
| User | 1.9 Integrated ICAM Platform | | | | | | | |
| Device | 2.1 Device Inventory | | | | | | | |
| Device | 2.2 Device Detection and Compliance | | | | | | | |
| Device | 2.3 Device Authorization w/ Real Time Inspection | | | | | | | |
| Device | 2.4 Remote Access | | | | | | | |
| Device | 2.5 Partially &Fully Automated Asset, Vulnerability and Patch Mgmt. | | | | | | | |
| Device | 2.6 Unified Endpoint Management (UEM) & Mobile Device Management (MDM) | | | | | | | |
| Device | 2.7 Endpoint & Extended Detection & Response (EDR & XDR) | | | | | | | |
| | 3.1 Application Inventory | | | | | | | |



Source: SSC/S6 ZT Self-Evaluation

# Inform ZT Capabilities with Assessment Data

Capabilities with 1:m activities merged

Target Activity ID and Response Provided

DAF Template Responses

Select the '+' sign above to expand the group and show results form the 7-pillar assessment

| | DoD ZT Capabilities | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | System Name: [] | | | | | | | | | |
| | DoD ZT Capability | Mapped DoD Target Activity (DATA PULLED FROM PILLAR WORKSHEETS) | Self-Evaluation Response (DATA PULLED FROM PILLAR WORKSHEETS) | Implementation Status | Expected Implementation Timeline | Leveraging Enterprise Implementation Solution (Yes/No) | Enterprise Implementation Tool or Solution | Additional Enterprise Implementation Tool or Solution | Implementation Approach | Additional Notes |
| User | 1.1 User Inventory | 1.1.1 - Inventory User | Complete | Complete | N/A | No | ICAM ID Provider | ICAM ID Governance | | |
| | 1.2 Conditional User Access | 1.2.1 - Implement App Based Permissions per Enterprise | In Process | Enterprise Solution Consideration | | | | | | |
| | | 1.2.2 - Rule Based Dynamic Access Pt1 | Not Started | | | | | | | |
| | 1.3 Multifactor Authentication | 1.3.1 - Organizational MFA/IDP | Complete | Complete | | | | | | |
| | 1.4 Privileged Access Mgmt. | 1.4.1 - Implement System and Migrate Privileged Users Pt1 | Complete | Complete | | | | | | |
| | | 1.4.2 - Implement System and Migrate Privileged Users Pt2 | N/A | | | | | | | |
| | 1.5 Identity Federation and User Credentialing | 1.5.1 - Organizational Identity Life- Cycle Management | Not Started | Delayed | | | | | | |
| | | 1.5.2 - Enterprise Identity Life-Cycle Management Pt 1 | In Process | | | | | | | |
| | 1.6 Behavioral, Contextual ID, & Biometrics | 1.6.1 - Implement User & Entity Behavior Activity (UEBA) and User Activity Monitoring (UAM) Tooling | Complete | Complete | | | | | | |
| | 1.7 Least Privileged Access | 1.7.1 - Deny User by Default Policy | Complete | Complete | | | | | | |
| | 1.8 Continuous Authentication | 1.8.1 - Single Authentication | In Process | Dependent on Another DAF ZT Capability | | | | | | |
| | | 1.8.2 - Periodic Authentication | Not Started | | | | | | | |
| | 1.9 Integrated ICAM Platform | 1.9.1 - Enterprise PKI/IDP Pt1 | N/A | Does Not Apply | | | | | | |

Source: SSC/S6 ZT Self-Evaluation

Basic Capabilities are informed by the ZT Target (and Advanced) activities, as such informed responses to capabilities require assessment of at least Target Level Activities

# Use Case

# ‘Unofficial’ Use Case

## NSA ZTMA Assessment with USSF PEO/System Owner

## **Goal:** Inform S6 ZT Self-Evaluation Framework

**Assessment Timelines:**

**.5 Day(s):**

Intro/Overviews

**1.5 Day(s)**

Pillar Assessments

**.5 Day(s)**

Prioritize and Schedule

**Process:**

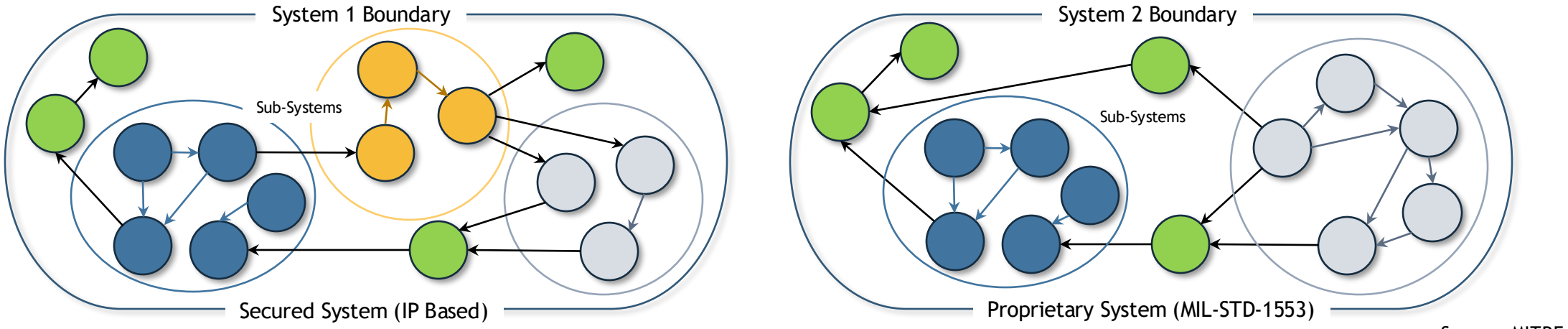
Focused ZT assessment with SMEs in a central location facilitated by an assessment team

| | |
|---|---|
| Day 1 | 0800-0830 Badging |
| | 0830-0900 Kick-Off - Introductions, rules, facilities |
| | 0900-1000 Zero Trust methodology overview / PEO Framework Overview |
| | 1000-1100 Pillar 1 |
| | 1100-1200 Lunch |
| | 1200-1300 Pillar 1 |
| | 1300-1600 Pillar 2 |
| Day 2 | 0800-0830 Badging |
| | 0830-1100 Pillars 3-4 |
| | 1100-1200 Lunch |
| | 1200 – 1600 Pillars 5-7 |
| Day 3 | 0800-0830 Badging |
| | 0830-1100 Analysis (Priority/Schedule) and Go-backs |
| | 1130-1200 Lunch - S6 Assessment Tool comparison (30 min) |
| | 1400-1500 Wrap-up/Out-brief |

# Decompose and Bound system(s)

Identify systems, subsystems, dependencies and critical dependencies

- Functional Decomposition




Source: MITRE

- Does the system 'resemble' tactical or enterprise system(s)?
- Inventory and deconstruct into subsystems, dependencies and critical dependencies

# Detour: Strategic Categorization

- Identify system characteristics to align to strategic categories
- Strategic Categories:
  - Secured IT System
  - Unsecured IT System
  - Standard OT System
  - Proprietary OT System
  - Disconnected System
- A guide for PEOs and AOs to:
  - Assess existing systems, subsystems, and dependencies, and
  - Determine a path forward to implement Zero Trust on those systems

Source: DAF I-Plan v.2 Draft, 1 Mar 25

# Returning to the 'Unofficial' Use Case

**Activity:** NSA ZTMA Assessment with USSF PEO/System Owner

**Goal:** Inform S6 ZT Self-Evaluation Framework

**Assessment Timelines:**

.5 Day(s):

Introductions and Overviews

**1.5 Day(s)**

Pillar Assessments to include Target and Advanced Activities

.5 Day(s)

Prioritize and Schedule Evaluation

**Process Analysis:**

The ability of having SMEs in the room for this event facilitated a timely assessment in 2.5 days

| | |
|---|---|
| Day 1 | 0800-0830 Badging |
| | 0830-0900 Kick-Off - Introductions, Run rules, facilities |
| | 0900-1000 Zero Trust methodology overview / PEO Framework Overview |
| | 1000-1100 Pillar 1 |
| | 1100-1200 Lunch |
| | 1200-1300 Pillar 1 |
| | 1300-1600 Pillar 2 |
| Day 2 | 0800-0830 Badging |
| | 0830-1100 Pillars 3-4 |
| | 1100-1200 Lunch |
| | 1200 – 1600 Pillars 5-7 |
| Day 3 | 0800-0830 Badging |
| | 0830-1100 Analysis (Priority/Schedule) and Go-backs |
| | 1130-1200 Lunch - S6 Assessment Tool comparison (30 min) |
| | 1400-1500 Wrap-up/Out-brief |

# Starts with Assessing Pillar Activities

Mark activities:

| | |
|---|---|
| Yes | Activity is complete |
| No | Activity not started, complete 'to-be' state |
| Partial | Activity in process, not fully complete |
| N/A | Activity does not apply to their system |

For activities marked partial:

| | |
|---|---|
| 'as-is' | Detail what is already accomplished in support of activity |
| 'to-be' | Identify actions needed to complete the activity |

Identify timeline to complete:

| | |
|---|---|
| Short | <3 months |
| Medium | 6-12 months |
| Long | > 1 year |

**NOTE:** Duration elements vary in staffing to complete, and each was determined by the system owner based on the staffing they felt could be allocated over the time span and was not always documented

# Returning to the 'Unofficial' Use Case

**Activity:** NSA ZTMA Assessment with USSF PEO/System Owner

**Goal:** Inform S6 ZT Self-Evaluation Framework

**Assessment Timelines:**

**.5 Day(s):**

Introductions and Overviews

**1.5 Day(s)**

Pillar Assessments to include Target and Advanced Activities

**.5 Day(s)**

Prioritize and Schedule Evaluation

**Process Analysis:**

The ability of having SMEs in the room for this event facilitated a timely assessment in 2.5 days

| | |
|---|---|
| Day 1 | 0800-0830 Badging |
| | 0830-0900 Kick-Off - Introductions, Run rules, facilities |
| | 0900-1000 Zero Trust methodology overview / PEO Framework Overview |
| | 1000-1100 Pillar 1 |
| | 1100-1200 Lunch |
| | 1200-1300 Pillar 1 |
| | 1300-1600 Pillar 2 |
| Day 2 | 0800-0830 Badging |
| | 0830-1100 Pillars 3-4 |
| | 1100-1200 Lunch |
| | 1200 – 1600 Pillars 5-7 |
| Day 3 | 0800-0830 Badging |
| | 0830-1100 Analysis (Priority/Schedule) and Go-backs |
| | 1130-1200 Lunch - S6 Assessment Tool comparison (30 min) |
| | 1400-1500 Wrap-up/Out-brief |

# Prioritization and Scheduling

Prioritization:

- ‘partial’ and ‘no’ responses evaluated using a 1-5 scale to identify priority
- All 152 activities reviewed and assessed

Scheduling:

- Selected a date in the future; ‘line in the sand’
- Established ‘starting’ point

Result: Final assessment with priority listing of activities and associated roadmap

S6 After Action Item

Validate SSC/S6 Self-Evaluation Framework using system owner outputs from the ZTMA assessment to inform S6 Self-Evaluation Framework

# Lessons Learned

# Lessons Learned

- **Complete ZT Assessment as a team:**
  - Identify a team responsible for ZT self-evaluation
  - Consider an off-site or seclusion to complete assessment
  - Include SMEs: mission owner, IT infrastructure engineer, cyber engineer, ZT SME, etc.

- **Determine the type and depth of assessment that fits your mission system**
  - Analyzing target activities prioritized to respond to the I-Plan
  - Next-Gen systems consider a full review (target & advanced activities)

# Use Case - Lessons Learned

Use Case Activity was a great learning opportunity

Two classes of information caused challenges for the team

1. Cyber Threat Intelligence (CTI)
2. Cybersecurity (DCO-S)

Majority of findings were partial completions

Very Few Not Applicable findings

Schedule and capabilities drove many prioritization decisions

Operational need or impact conversations were continual

# Questions

- **Integration Questions**
  - Will DAF require mission system to integrate with DAF/SSC level ICAM?
  - Will DAF require mission system to integrate with DAF/SSC level PDP?
    - What is the best approach to deploy a local PDP if integration is not possible?

- **How to help mission systems select optimal ZT capabilities**
  - ZT capabilities that can integrate into existing infrastructure
  - Co-existence with other cyber products should be evaluated

- **SSC/S6 Vendor Evaluation Framework**
  - Framework to serve SSC mission systems to assist with down-select capabilities and vendors for each of the core/supporting areas in ZT as needed

# SSC/S6 Vendor Evaluation Framework

## Space Systems Zero Trust Principles

### ZERO-TRUST PRINCIPLES

- Assume no implicit or explicit trusted zone in networks.
- Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.
- Machine to machine (M2M) authentication and authorization are strictly enforced for communication between servers and the applications.
- Risk profiles, generated in near-real-time from monitoring and assessment of both user and devices behaviors, are used in authorizing users and devices to resources.
- All sensitive data is encrypted both in transit and at rest.
- All events are to be continuously monitored, collected, stored, and analyzed to assess compliance with security policies.
- Policy management and distribution is centralized
- Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction.

### ZT WEAPON SYSTEMS AND DEFENSE CRITICAL INFRASTRUCTURE MISSION PRINCIPLES

- Resilient – the capacity to withstand or to recover quickly from difficulties
- Effective – the degree to which something is successful in producing a desired result
- Reliable – the quality of being trustworthy and performing consistently
- Safe – protected from or unlikely to cause danger, risk or injury
- Sustainable – the ability to be maintained at a certain rate or level
- Adaptable – the ability to adjust to changing conditions
- Observable – the ability to measure the internal state of a system
- Secure – to reduce the risk of threats, intrusion and attacks.
- Dynamic Configurability - Flexibility to configure system-level changes such as governance, trust relationships, workflows, or access policies to implement ZT capabilities (or WS-adapted ZT architectures) in near real time.
- Design/Retrofit Flexibility - Flexibility to change the engineering design or retrofit existing system to implement ZT capabilities.
- SWaP - Size, weight, and power constraints that impact the ability to change the engineering design or make changes to the operational system to implement ZT capabilities (or WS adapted ZT architectures).
- Latency Tolerance - Ability to absorb delay introduced by ZT capabilities (or WS-adapted ZT architectures) and still meet system performance requirements
- IT/OT-centricity - The makeup of computing components to include traditional Itcentric devices, OT devices and controllers, or combinations of both.

## SSC S6 Vendor Evaluation Framework ZT Analysis (June 30th, 2025)

### Eco Systems

#### IT SYSTEMS

- Cloud, On-Premises, Hybrid, Edge
- OCONUS, CONUS

#### Non-IT SYSTEMS

- Ground Segment, User Segment, Space Segment
- Other Non-IT Systems

### DoD Capabilities

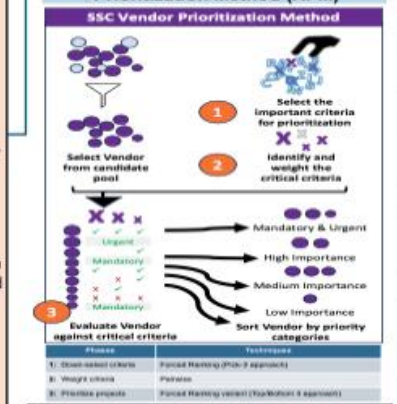
#### DAF ZT Capabilities

- DAF EIT FMO Capabilities and Roadmap
- CloudONE
- PlatformONE
- CLOUDworks
- NIPRGPT
- DAF OT ZT Pilots

#### DoD and Partner Agencies ZT Capabilities

- DISA Thunderdome
- C5ISR Capabilities
- SBIRs
- Other Partner ZT Capabilities

### Vendor Selection Rapid Prioritization Method (RPM)




- Timing: <X> days> based on # of prioritization objects
- Scoring: 1 – 6 For objective forced choice scoring selection

### SSC ZT Needs

#### SSC Program Priorities

- Niche vs. Common ZT product strengths
- API Integration
- Tool Coupling and Cohesion dependencies
- SecOPS and DevSecOps Integration
- Tagging Strategies
- Agent based vs. Agentless
- Discovery & Inventory Integration strategies
- SIEM & AI/ML integration capabilities
- Deployment strategies
- Micro-services, SDN, and Macro-services strategies
- Kubernetes, Cloud, Edge and On-Prem integrations
- Training & Skills needed for support
- Person, non-person-entities (NPE), M2M, mTLS and other protocols
- Threat Centric ZT Integration
- Application and Workload ZT Integration
- Data Centric ZT Integration
- Network Centric ZT Integration
- User and NPE Centric ZT Integration
- Device Centric ZT Integration
- Policy Centric ZT Integration
- AI/ML and Analytics Centric ZT Integration
- Vulnerability Centric ZT Integration
- API Centric ZT Integration
- Automation and Orchestration Centric ZT Integration
- Edge Centric ZT Integration
- Infrastructure Centric ZT Integration
- Tools Integration Centric ZT Integration
- Ecosystem Centric ZT Integration
- Operations and Management Centric ZT Integration
- Mission Centric ZT Integration
- People, Process and Governance Centric ZT Integration
- Planned or On-going Program Modernization Efforts

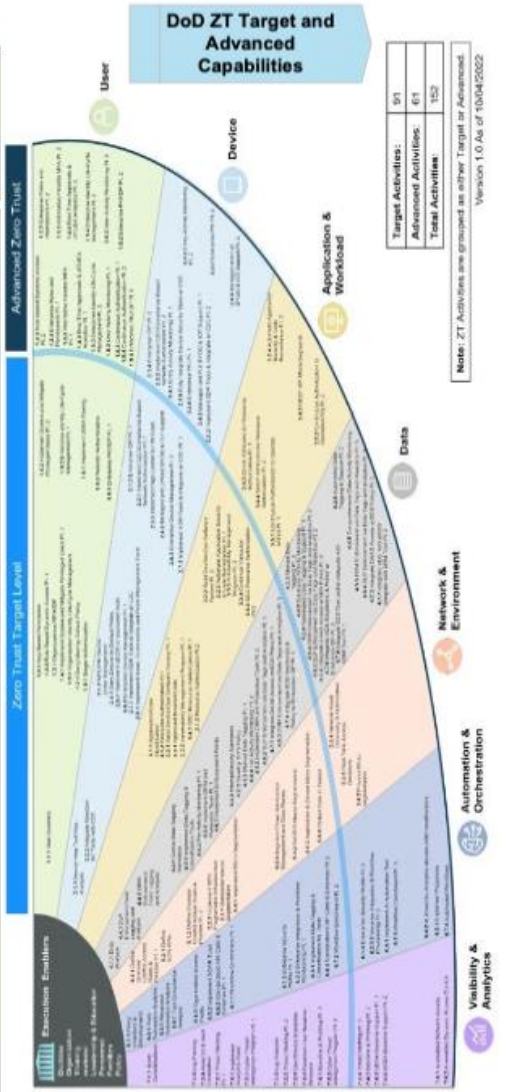
#### SSC ZT Planning

- SSC ZT Roadmap
- SSC ZT Program Gaps
- SSC Risk Mitigation
- SSC ZT Vendor Catalog
- SSC ZT Acquisition Strategy

#### SSC Governance ZT Factors

- Threat Intelligence & Alerting
- Threat Coordination and Cyber feeds integration
- Ephemeral vs. Static Rules enforcements
- ZT DAF Capabilities
- Dynamic Policy, Groups & Rules enforcements
- Logging, Auditing, Alerting & Monitoring
- Just-in-Time-Actions and Just-enough-Administration
- Continuous Adaptive Risk and Trust Management
- Data Plane and Control Plane Segmentation
- Vendor acquisition, SLAs, Contracts, and Pricing
- Enterprise Tool compatibility and integrations
- Integrated ZT Comprehensiveness
- Product Integration
- IDS & IPS capabilities
- SecOPS and DevSecOps Integration
- Configuration Management strategies
- Tool Chattiness
- Performance KPIs
- Recovery and Availability
- Confidentiality and Integrity
- DoD, NIST and other standards compliance
- Patching and Vulnerabilities
- Supply Chain and SBOM
- Product Robustness and Stability
- License models and License costs
- Fine-grain access, ABAC and RBAC integrations

### DoD ZT Target and Advanced Capabilities



# Way Ahead

- Identify assessment tools to assist system owners
- Continue work on SSC/S6 vendor evaluation framework
- Continue to track DoD/DAF activities to inform SSC/S6 actions
- Determine tracking methodologies to support ZT mandate (KPPs/KPIs)
- Collaborate, coordinate, and integrate to ensure adoption

# Space Systems Command (SSC)
# S6 Communications

## Questions?

**Maj. Min Kang**
Acting Cybersecurity Division Chief
min.kang.5@spaceforce.mil

**Chad Korosec**
ZT Support to SSC/S6
ckorosec@mitre.org