2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

WELCOME TO

Day 2 | Wednesday April 22

Mission Application: Strategy Set. Mission Go!

event website

Cyber Readiness at the Speed of Space

Day 2: Mission Application: Strategy Set. Mission Go!

Morning Schedule

- 0900 - 0905 Introductions
- 0905 - 0940 Leadership Address—Dr. Keith Hardiman
- 0940 - 1015 Keynote Address—Mr. John Weiler
- 1015 - 1030 Break! Visit Exhibitors
- 1030 - 1145 DAF Zero Trust Lightning Talks outline current and future intent of "Never Trust, Always Verify" framework, building the foundation of a resilient, digital backbone:
  1. DAF Zero Trust Functional Management Office
  2. National Institute of Standards & Technology
  3. Self Evaluation for Mission Systems
  4. Vendor Framework
  5. Zero Trust Defense in Space Satellite Development
- 1145 - 1245 **Lunch**

✦ Special Guest Speaker ✉ SSC.S6.CyberExpo@spaceforce.mil

Cyber Readiness at the Speed of Space

Day 2: Mission Application: Strategy Set. Mission Go!

Afternoon Schedule

- 1245 - 1300 Authority to Operate
- 1300 - 1320 Project Enigma: Satellite Communications Digital Cloud Environment
- 1320 - 1345 Program Protection & Supply Chain Risk Management
- 1345 - 1355 Break! Visit Exhibitors
- 1355 - 1415 Defensive Cyber Operations for Space
- 1415 - 1435 Delivering Cybersecurity Service Provider (CSSP) Capabilities
- 1435 - 1455 On-Orbit Cyber Defense: Secure by-Design Space Vehicles
- 1455 - 1505 Break! Visit Exhibitors
- 1505 - 1520 Judgement Under Operational Pressure
- 1520 - 1545 Innovation Lab: Accelerating Innovation for the Warfighter
- 1545 Closing Remarks
- 1545 - 1730 Network Social @South Bay Bar & Grill

Questions? Contact us ✉ SSC.S6.CyberExpo@spaceforce.mil

Cyber Readiness at the Speed of Space

SOUTH BAY BAR & GRILL

Drink Voucher Sponsors

August Schell

Google

Illumio

NetScout

Red River

Rise8

MoonTiger

Viasat

VioletX

Space Force Association

2026 SSC CYBER EXPO

Department of the Air Force Leadership Address

Dr. Keith Hardiman
Deputy Director, DAF Chief Information Office

Cyber Readiness at the Speed of Space

Introduction

- **Dr. Keith L. Hardiman**
  - DAF Deputy Chief Information Officer

DAF CIO Strategy Snapshot

INTRO

This strategy seeks to operationalize Federal Title Authorities through agile governance, optimized investments, proactive risk management, and decisive empowerment. By modernizing DAF IT infrastructure and defense business systems, strengthening cybersecurity, reducing cost, and accelerating innovation, the DAF CIO will deliver a digital enterprise where IT is a decisive contributor to lethality, readiness, and mission success.

LOE 1: ENABLING MISSION AGILITY

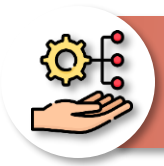
Deliver modern capabilities to the warfighter and maximize efficiency

DESCRIPTORS: Unified Cloud | DevSecOps | Divest to Reinvest | Hybrid and Edge | Modernize Connectivity | Accelerate DBS

LOE 2: SCALING CYBERSECURITY THROUGH THE LIFECYCLE

Continuously enhance a secure and resilient digital environment

DESCRIPTORS: Risk Awareness | Automated Visibility & Instrumentation | Risk Management | Zero Trust & ICAM | Resiliency | DBS Audit & IT Control



LOE 3: OPTIMIZING THE WORKFORCE

Develop strategic talent within the DAF Civilian workforce to meet and adapt to mission demands

DESCRIPTORS: Enhancing Joint Workforce | Talent Management | Digital Learning | Cyber Workforce Framework Alignment | Workforce of the Future

LOE 4: INTEROPERABILITY THROUGH GOVERNANCE & COMPLIANCE

Maximize the value of DAF IT investments

DESCRIPTORS: Strategic Oversight | Financial Stewardship | Portfolio Optimization | Policy, Compliance, & Governance | Category Management

LOE 5: ACCELERATING DATA & AI

Unleash the power of data and AI for information dominance and operational superiority

DESCRIPTORS: Scalable Data & AI | Data on Demand | Lawful Data & AI Governance | AI Innovation | Advance the Workforce

STRATEGIC AIM

Deliver streamlined, secure, and warfighter-focused IT that increases lethality, enhances readiness, accelerates acquisition, reduces cost, and empowers Airmen, Guardians and Civilian Professionals to fight and win across all domains.

Questions?

Thank You!

For more information, please contact:

SAF CN Front Office

Email: SAF.CN.Workflow@us.af.mil

2026 SSC CYBER EXPO

Keynote Address

Discerning the multiple dimensions of risk with commercial IT solutions (COTS) based platforms

Mr. John Weiler

CoFounder and CEO of the IT Acquisition Advisory Council, will present his insights on challenges and opportunities relating to assessing the many dimensions of risk associated with commercial IT (COTS, Cloud, SaaS)

John A. Weiler

Co-Founder and Executive Director,

IT Acquisition Advisory Council

(an ICH managed Public/Private Partnership)

The influx of commercial IT into DOW has never been greater, neither has the growing cyber attacks on commercial IT infrastructure (COTS, Cloud, Networks), forcing DOW PMs to rethink traditional risk assessment approaches that enable greater information sharing and collaboration.

Assessing Risks in Commercial Items

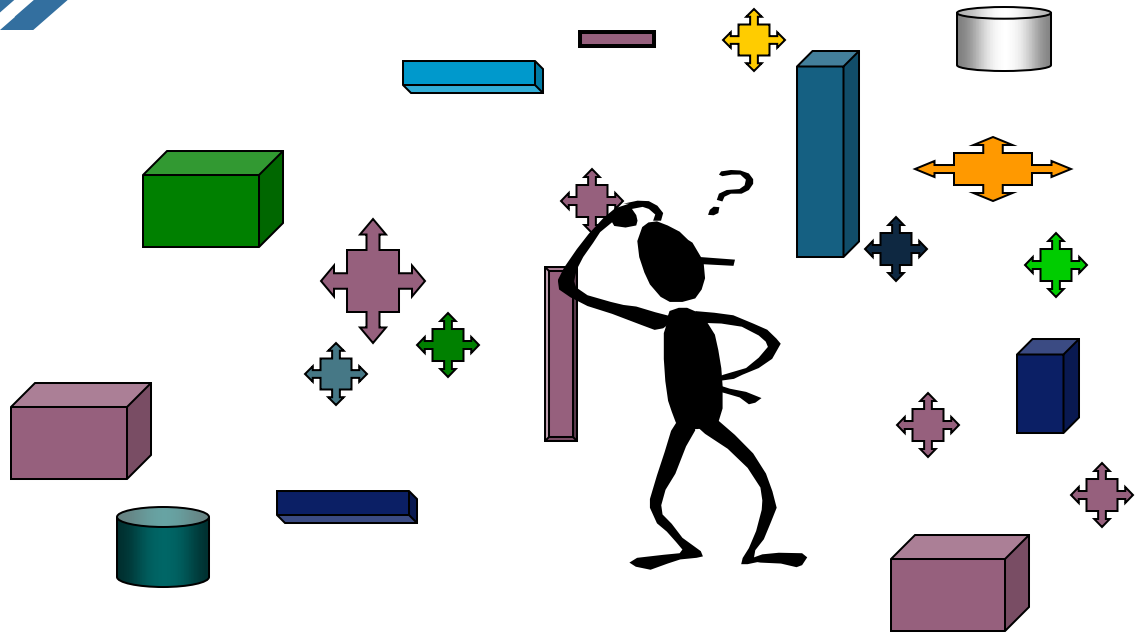
The commercial IT/AI/Cyber market is exploding with both innovations and risk.

- PM's are facing the dual challenges of increased rate of IT innovation and growing AI enabled cyber threats.
- PM and Agency CxOs must also answer the many legislative mandates including Clinger Cohen Act, FISMA, FITARA, and EO14265, leaving little time to conduct "green fields research" when resources are already stretched thin meeting mission priorities.
- Delayed and mis-managed IT modernization efforts are keeping legacy systems that drain resources and are rife with known cyber vulnerabilities that are under persistent attacks.

Interop. Clearinghouse | John Weiler, CEO john@ICHnet.org, Executive Director of the IT Acquisition Advisory Council john.weiler@IT-AAC.org | 703-863-3766

Managing Complexity and speed of COTS

PMs Feel increasingly overwhelmed…



by Complexity,
Ill-equipped to evaluate COTS risk,
Over Hyped Suppliers,
Compliance vs Outcomes?
Conflicted ?

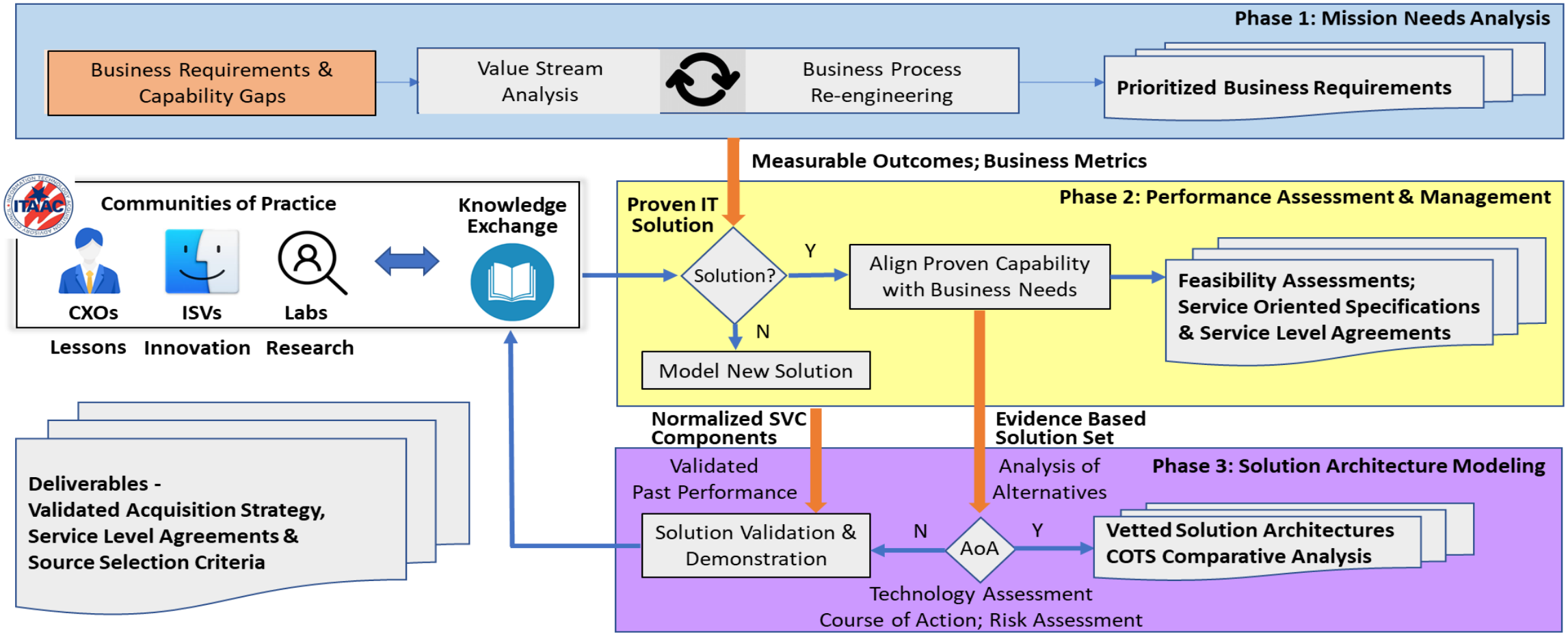
- **Fast paced IT market undermines traditional research efforts.**
- **Mountains of Legislative Directives relating to COTS, SCRM, ZTA, CMMC, and Cyber Resilience**
- **Green Fields testing takes too long and cost too much**
- **No Clearinghouse of shared testing results emanating out of Fortune500 or Silicon Valley**
- **No legal mechanism of assessing emerging COTS outside of existing contracts**
- **Traditional Check List processes take too long and don't address real risk.**

Aligning Resources with Rule of Law and Mission Needs

Partner Type Federal IT Lifecycle	FFRDC	User Groups, Communities of Practice	Standards development Orgs, Trade Associations	Public Private Partnerships	Consultants, IV&V, A&AS Firms	Innovators, Tech Mfg, Open Source	System Integrators
Requirement, Gap Analysis, Innovation Research	Lacks access to commercial innovations or best practices	OMB Lines of Business offers Critical Role	SDOs = Primary driver for open systems. Conflict free structures	Provide Conflict free structure and economies of scale	Limited access to industry lessons learned.	Great source for customer use cases, lessons learned.	FAR 9.5 OCI Rules limit participation
MOSA/OSI Planning	Only when no other company can support	Agency CXO provides critical guidance	Provide standards of practice, not support	Principle source of expertise. Organic access to standards	Primary source of expertise, but requires access to Standards	FAR OCI rules limit participation	FAR OCI rules prohibit direct support
PMO & IV&V Support	Only when no other company can support	Not inherently Governmental	Access to standards of practice of suppliers	Optimized for this area	Key role	FAR OCI rules prohibit participation	FAR OCI rules prohibit participation
Solution Engineering	FAR Part35 prohibits use if available from other sources	Not inherently Governmental	Access to potential suppliers already in market	Support role, provide process standards, lessons learned	Support role	Provide developmental	Primary partnership area
Performance Management & Acqusition	Forbidden, may not develop material solutions	Not inherently Governmental	Potential OCI, objectivity	ICH/IT-AAC does not develop, sell, or integrate any IT	Internal IV&V for Prime contract reduces risk.	Provider of key technologies	Primary partnership area

DOW is just 1% of the Global IT Market

Thus demanding that DOW PMs improve cyber information sharing and collaboration with the other 99% of the market



DOW Tech Proving Grounds P3

DIU Initiated, ARL Hosted, IT-AAC Managed

IT-AAC Partners	Agile Methods	Cloud/HCI	Innovation Access	IT Risk Mgmt	Industry Best Practices	Pilots & Contracts	IT Policy & Compliance	#Companies (SMEs)
ANSER Corp		✓	✓		✓	✓	✓	325+
CMU Cylab		✓	✓	✓	✓	✓		150+
Cloud Security Alliance (CSA)	✓	✓	✓	✓	✓	✓	✓	48,000
USU Space Dynamics Lab	✓		✓	✓	✓	✓		750+
Interoperability Clearinghouse (ICH)	✓	✓	✓	✓	✓		✓ ✓	360
Info Systems & Security Group (ISSA)			✓	✓	✓	✓	✓	10,000+
Object Mgmt Group Industrial Internet Consortium		✓	✓	✓	✓	✓		800+ 250+
OMG/Digital Twins	✓		✓	✓	✓	✓		1,600+
HyperQube		✓	✓		✓		✓	1,100
Consortium for Information and Software Quality (CISQ)	✓		✓	✓	✓	✓	✓	600+
Telecommunication Industry Association (TIA)								290+
MISI Dreamport								100+

The MITRE Corporation: "the concept of the Interoperability Clearinghouse is sound and vital. Its developing role as an honest broker of all interoperability technologies, no matter what the source, is especially needed. Such efforts should be supported by any organization that wants to stop putting all of its money into maintaining archaic software and obtuse data formats, and instead start focusing on bottom-line issues of productivity and cost-effective use of information technology."

Questions?

We at the Interoperability Clearinghouse (ICH), and our IT-AAC public service partners, have invested decades in improving the state of Federal IT, and welcome the opportunity to leverage the significant investments of our public services partners who stand ready to help facilitate tech transformation thru the infamous “valley of death”. Our collective work brings a unique mix of international standards, Fortune500/Silicon Valley Innovations, Physical Testing Labs and World Class Domain Experts willing to mentor and facilitate the adoption of mission critical technology at the speed of relevance.

DOD, GSA, IC and DHS have already embraced a suite of alternative, agile DevOps processes and innovation research capabilities that have been underutilized due to DOD’s bureaucratic barriers to change and unwillingness to take the extra effort to embrace alternative methods or sources of expertise outside the confines of the Defense Industrial Base. As DOD’s primary champion of innovation, we recommend that NCD establish a Partnership Intermediary Agreement that closes the SCRM gaps leveraging a wide range of non-profits working in the public interests.

Thank You!

For more information, please contact:

John Weiler
Executive Director, CoFounder IT-AAC
Member, DOW BOND
John.weiler@IT-AAC.org
CEO, Interop. Clearinghouse
john@ICHnet.org
703-863-3766
www.IT-AAC.org/DOGE

2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

BREAK

VISIT EXHIBITORS!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Zero Trust Lightning Talks

Moderator: Mr. Mark Munoz, SSC/S6 Cyber Security Resiliency Specialist

LT #1 - DAF Zero Trust Functional Management Office (FMO), Capt Kristen Walsh

LT #2 – National Institute of Standards & Tech., Dr. Parisa Grayeli, MITRE

LT #3 - Self Evaluation for Mission Systems, Nedu Irrechukwu, MITRE

LT #4 - Vendor Framework, Dr. Safwa Ameer, MITRE

LT #5 - Zero Trust Defense in Space Satellite Development, Mr. Nick Cohen, Aerospace

DAF ZERO TRUST FUNCTIONAL MANAGEMENT OFFICE

DAF Zero Trust Update

Capt Kristen Walsh

22 APR 2026

Agenda

1 *DAF ZT 101 & History*

2 *DAF ZT Solutioning*

3 *Year in Review, Way Forward*

4 *DoW ZT PfMO Purple Team & Planning Efforts*

ZT 101 | *Zero Trust Definition and Mission*

Zero Trust focuses on the mission, rather than the network.

Zero Trust is a data/application access strategy that…

- ✓ Assumes all resource requests originate from an untrusted source
- ✓ Grants access for each request after confidence, in both the user and device, is established through identity verification and connection context attributes
- ✓ Assumes compromise so the security policies and TTPs must change to meet this strategic mindset

Continuous monitoring and validation

Assumes conditions of trust can change at any point

Extends beyond user authentication

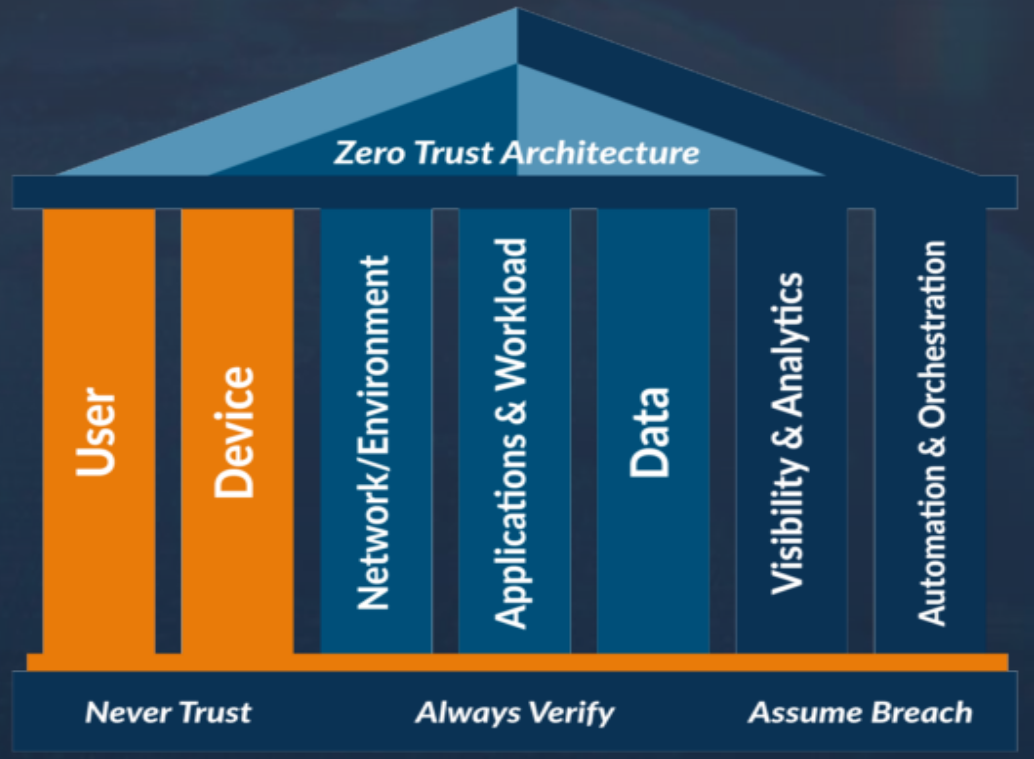
Also assesses device integrity across managed and unmanaged end user devices

Attribute-based

Explicitly implements principle of least privilege and data compartmentalization

Infers multiple levels of confidence

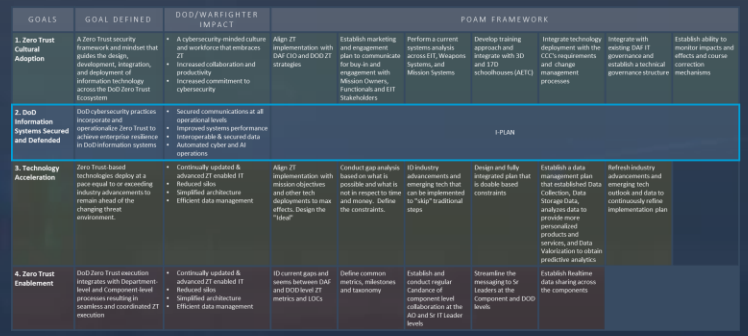
Dynamic granular access to resources derived from session context



ZT 101 | *Zero Trust Strategic Guidance*

The DAF ZT FMO leveraged both DoD-level and DAF-level ZT Guidance documents when building out the ZT Implementation Plan.

DOD ZT GOALS & POAM



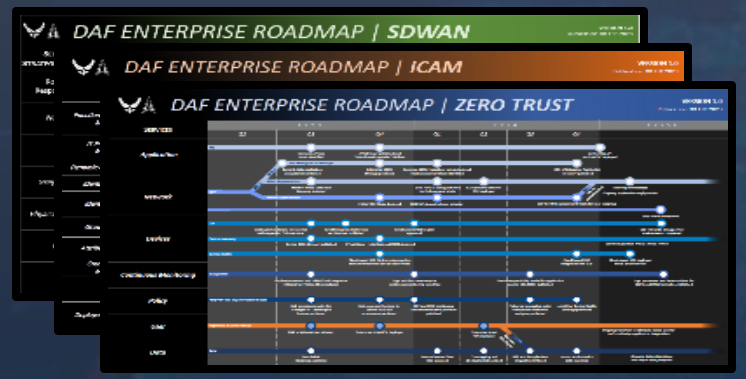
GOALS	GOAL DEFINED	DOD/WARFIGHTER IMPACT	POAM FRAMEWORK						
1. Zero Trust Cultural Adoption	A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem	• A cybersecurity-minded culture and workforce that embraces ZT • Increased collaboration and productivity • Increased commitment to cybersecurity	Align ZT implementation with DAF CIO and DOD ZT strategies	Establish marketing and engagement plan to communicate for buy-in and engagement with Mission Owners, Functionals and EIT Stakeholders	Perform a current systems analysis across EIT, Weapons Systems, and Mission Systems	Develop training approach and integrate with 3D and 17D schoolhouses (AETC)	Integrate technology deployment with the CCCs requirements and change management processes	Integrate with existing DAF IT governance and establish a technical governance structure	Establish ability to monitor impacts and effects and course correction mechanisms
2. DoD Information Systems Secured and Defended	DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD Information systems	• Secured communications at all operational levels • Improved systems performance • Interoperable & secured data • Automated cyber and AI operations	I-PLAN						
3. Technology Acceleration	Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment.	• Continually updated & advanced ZT enabled IT • Reduced silos • Simplified architecture • Efficient data management	Align ZT implementation with mission objectives and other tech deployments to max effects. Design the "Ideal"	Conduct gap analysis based on what is possible and what is not in respect to time and money. Define the constraints.	ID industry advancements and emerging tech that can be implemented to "skip" traditional steps	Design and fully integrated plan that is doable based constraints	Establish a data management plan that established Data Collection, Data Storage Data, analysis data to provide more personalized products and services, and Data Valorization to obtain predictive analytics	Refresh industry advancements and emerging tech outlook and data to continuously refine implementation plan	
4. Zero Trust Enablement	DoD Zero Trust execution integrates with Department-level and Component level processes resulting in seamless and coordinated ZT execution	• Continually updated & advanced ZT enabled IT • Reduced silos • Simplified architecture • Efficient data management	ID current gaps and seems between DAF and DOD level ZT metrics and LOEs	Define common metrics, milestones and taxonomy	Establish and conduct regular Cardance of component level collaboration at the AO and Sr IT Leader levels	Streamline the messaging to Sr Leaders at the Component and DOD levels	Establish Realtime data-sharing across the components		

Description:

The DoD ZT PfMO outlined 4 ZT goals for a department level ZT adoption and implementation that the DAF ZT FMO team translated into a POAM framework. The 4 goals are listed below:

1. Zero Trust Cultural Adoption
2. DoD Information Systems Secured and Defended *(Implementation Plan)*
3. Technology Acceleration
4. Zero Trust Enablement

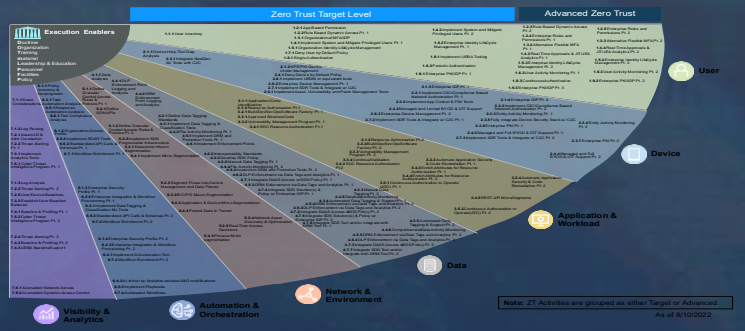
DAF CIO STRATEGIC ROADMAPS



Description:

The SAF/CN team under the direction of the DAF CTO, developed strategic-level roadmaps for DAF Zero Trust implementation. It is built in alignment with DoD Architecture and intended to be updated on a quarterly basis.

DOD ZT FAN CHART



Description:

The DoD ZT Architecture to include 7 capability pillars, 42 capabilities, and 152 services/activities. The DAF ZT FMO and DAF are working to align status updates, reporting, and task management frameworks to this list of mandates.

ZT 101 | *Where We've Been and Where We're Going*

Zero Trust focuses on the mission, rather than the network.

WHAT'S BEEN DONE SO FAR

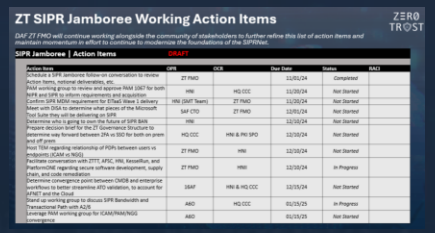
DAF ZT EIT I-Plan Jamboree(s)

JUN 2023

Brought ZT stakeholders together to discuss tasks, timelines, and OPRs for EIT ZT Milestones

ZT SIPR Gap Assessment & Jamboree

Outlined a plan and action items with activities, dates, and OPRs for ZT implementation on SIPR



ZT I-Plan 2.0 SECAF Glassdoor

Seeking SECAF approval for required activities to implement ZT in EIT and Non-EIT Environments (and held Non-EIT Summit)

DEC 2024

ZT Cloud Wall Walk

Identified ZT Cloud Capability alignment to DoD ZT Mandate Pillars with key stakeholders to confirm accuracy

IPLAN 2.0 Scope

Non-EIT

Shifting focus to Non-EIT in I-Plan 2.0. The DoD plans to release an OT Fanchart in Fall 2025

NEXT STEPS

Refocused DoD Alignment

Scheduling of acceptance criteria (purple testing), acquisition/rollout/integration of NGG, ICAM, C2C, etc.

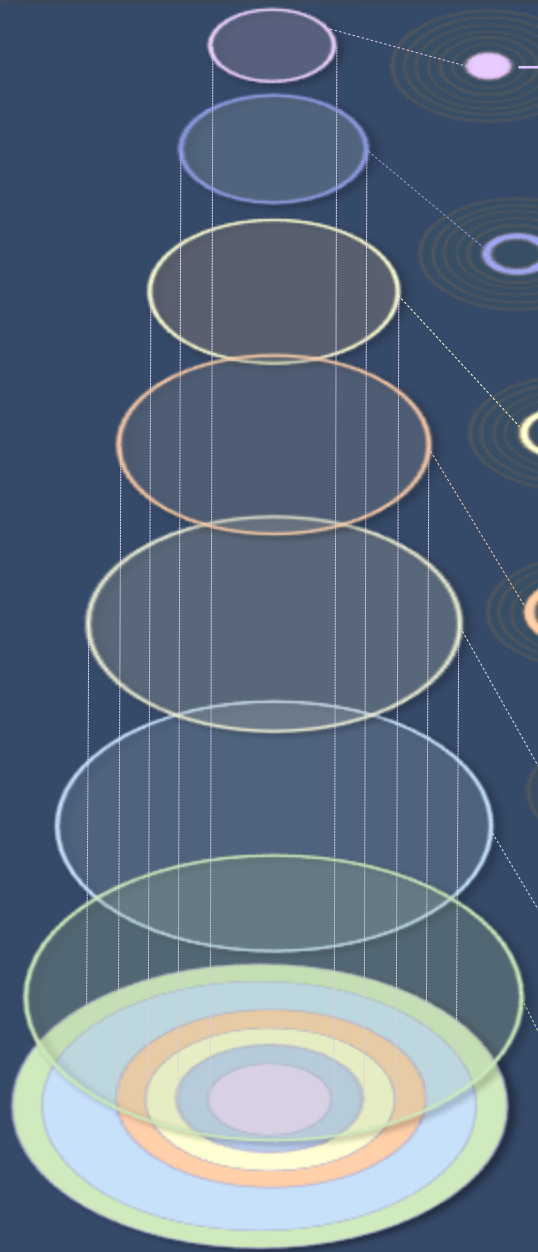
Operationalizing Zero Trust in the DAF

ZERO TRUST

DoD ZT STRATEGY

91 Target Activities are to be completed by end of FY 2027.

The “fan chart” structures DoD ZT into 7 Pillars, 91 Target Activities, and 61 Advanced Activities.



Visibility & Analytics

- Capabilities: 6
- Target Activities: 12
- Advanced Activities: 6

Automation & Orchestration

- Capabilities: 7
- Target Activities: 13
- Advanced Activities: 7

Applications & Workload

- Capabilities: 5
- Target Activities: 12
- Advanced Activities: 6

Network & Environment

- Capabilities: 4
- Target Activities: 10
- Advanced Activities: 3

Data

- Capabilities: 7
- Target Activities: 17
- Advanced Activities: 14

Device

- Capabilities: 7
- Target Activities: 14
- Advanced Activities: 10

User

- Capabilities: 9
- Target Activities: 13
- Advanced Activities: 15

DAF ZT REQUIREMENTS & PROJECTS:

Visibility & Analytics	• Log Parsing & Analysis • SIEM (IDCS + Sentinel) • Behavioral Analytics (UEBA) • Threat Intelligence	• Enterprise Logging • CTI Data Feeds
Automation & Orchestration	• PDP/PEP (NIST SP 800-207) • AI/ML • SOAR (IDCS + Sentinel) • API Standardization	• Enterprise API Services • CSSP & SOC R&R
Applications & Workload	• DevSecOps • CI/CD Pipelines • Software Defined Compute • Vulnerability Management	• Application Inventory • SBOM • Resource Authorization gateways
Network & Environment	• Macrosegmentation • Microsegmentation • Software Defined Perimeter (SDP)	• Software Defined Networking • Access Control Rules • Data in Transit
Data	• Data Standards • Data Mesh Environment • Data Tagging/Classification • Data Loss Prevention • Software Defined Storage	• Data Rights Management • File Activity Monitoring
Device	• Comply-To-Connect (C2C) • Mobile Device Management • Unified Endpoint Management (UEM)	• Config Mgmt Database (CMDB) • Detection & Response (EDR/XDR)
User	• Identity, Credential, Access Management (ICAM) • UEBA & User Activity monitoring	• Privileged Access Management • Dynamic Access Rules

Year in Review: Orchestrating Efforts and Execution

ZERO TRUST

Challenges

- Mapping what we currently have
- Aligning to the ZT Fan Chart
- Policy Orchestration
- Communicating ZT requirements
- Reporting on mission systems
- Decentralized Comply-to-Connect
- Integration, Integration, Integration

Good News Stories

- E5 Implementation in O365
- Application Microsegmentation
- OT Pilots: Spangdahlem, Chinook Test Lab, BAH Arnold
- DoW Approved ICAM Solution
- Purple Teams On-track: Scott AFB, Cloud One

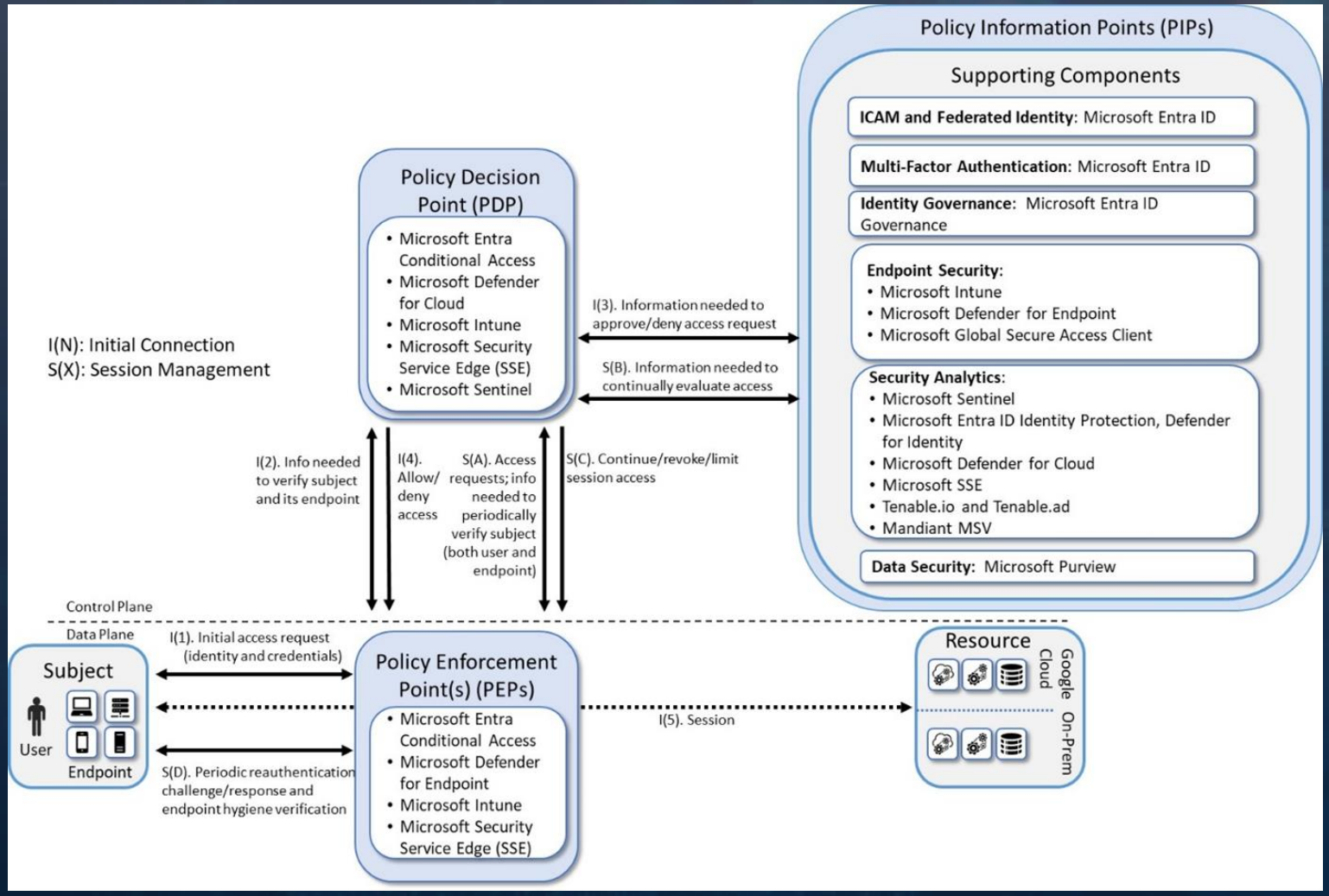
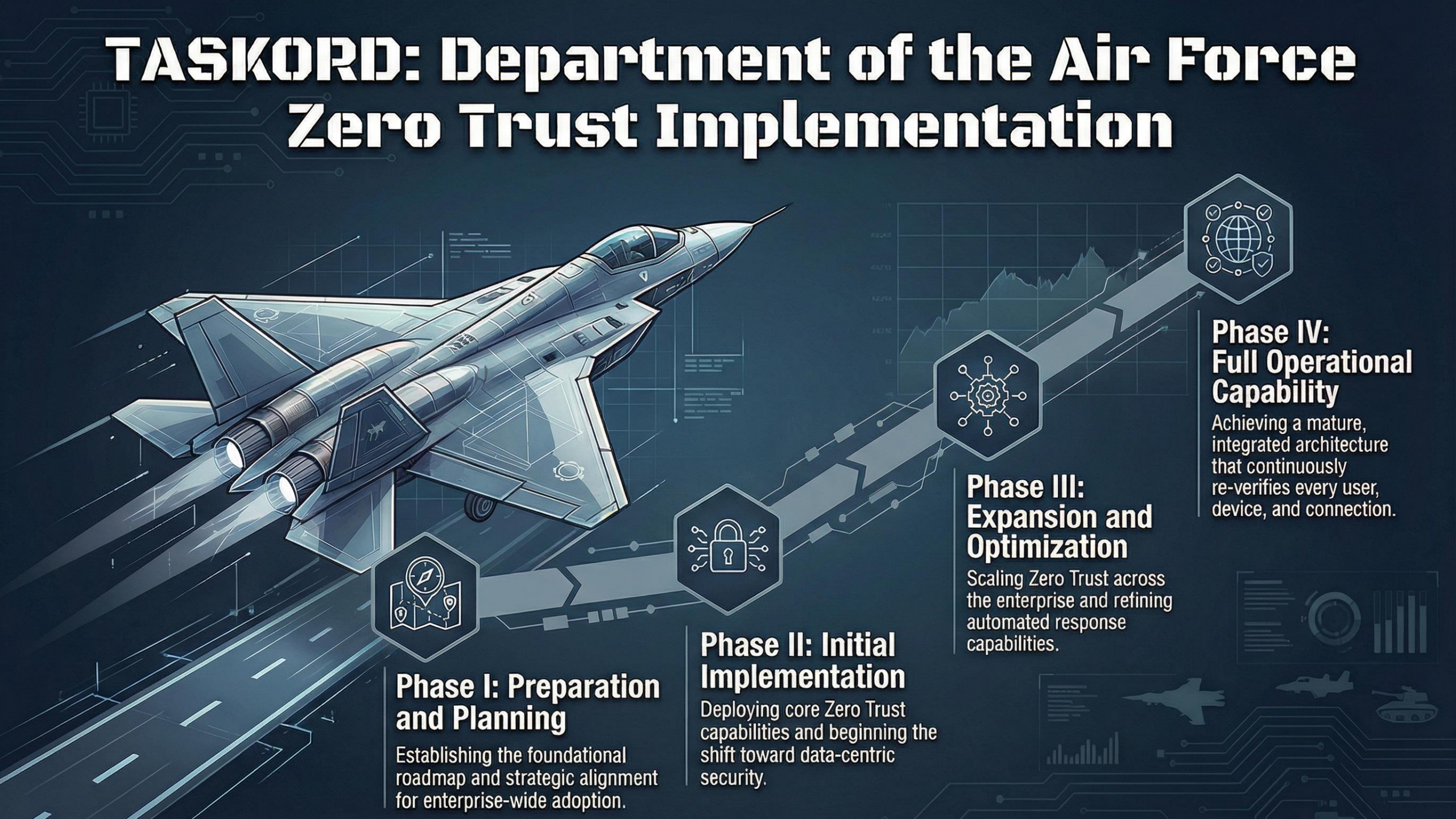


Figure 1 - Logical Architecture of E3B5 (NIST SP 1800-35: Implementing a Zero Trust Architecture)

TASKORD: Department of the Air Force Zero Trust Implementation



Phase I: Preparation and Planning

Establishing the foundational roadmap and strategic alignment for enterprise-wide adoption.

Phase II: Initial Implementation

Deploying core Zero Trust capabilities and beginning the shift toward data-centric security.

Phase III: Expansion and Optimization

Scaling Zero Trust across the enterprise and refining automated response capabilities.

Phase IV: Full Operational Capability

Achieving a mature, integrated architecture that continuously re-verifies every user, device, and connection.

Purple Team Assessment:

How does Target or Advanced ZT actually get "validated"?

ZERO TRUST

3 Step Self-Assessment Process *(PASS/FAIL)*

+

10-step ZT Acceptance Criteria *(PASS/FAIL)*

+

91/152 Independent Purple Team Assessment Results

=

ZT Target or Advanced level ZT *validation* by DoD CIO//ZT PfMO
[Must demonstrate stopping adversary freedom of movement]

1. **YOU ARE WHO YOU SAY YOU ARE**
   - Continuous authentication and credentialing.
2. **YOU ARE AFFIRMED TO ASSUME A ROLE**
   - Authorization, verification, and validation.
3. **ROLE ASSUMED IS SPECIFIED**
   - Attribution and behavioral rules.
4. **RESOURCES ARE ASCRIBED W/ OPERATING CHARACTERIZATIONS**
   - Attribution.
5. **ASSETS ARE ASCRIBED W/ ACCESS & USE CHARACTERIZATIONS**
   - When, where, and how information is allowed for use.
6. **POLICY IS SPECIFIED TO DICTATE ACTIONS**
   - Rules.
7. **IBAC/RBAC/ABAC IS CONSISTENT & VALIDATED**
   - Rules are consistent, coherent, complete, and validated.
8. **ENFORCEMENT SERVICES CAN APPLY ZT DETERMINATIONS ACCURATELY**
   - Continuous authentication and credentialing.
9. **BEHAVIORAL ANALYTICS TRACK AND EVALUATE PATTERNS**
   - ML/AI.
10. **UNANTICIPATED CONDITIONS ESCALATED**
    - Immediately for accommodation.

Questions?

2026 SSC CYBER EXPO

Implementing a Zero Trust Architecture (ZTA)

National Institute of Standards and Technology (NIST)
National Cybersecurity Center of Excellence (NCCoE)

Dr. Parisa Grayeli

Principal Cybersecurity Engineer

The MITRE Corporation

Agenda

- NIST NCCoE Overview
- NCCoE ZTA Project
- NCCoE DevSecOps Project

National Cybersecurity Center of Excellence (NCCoE)

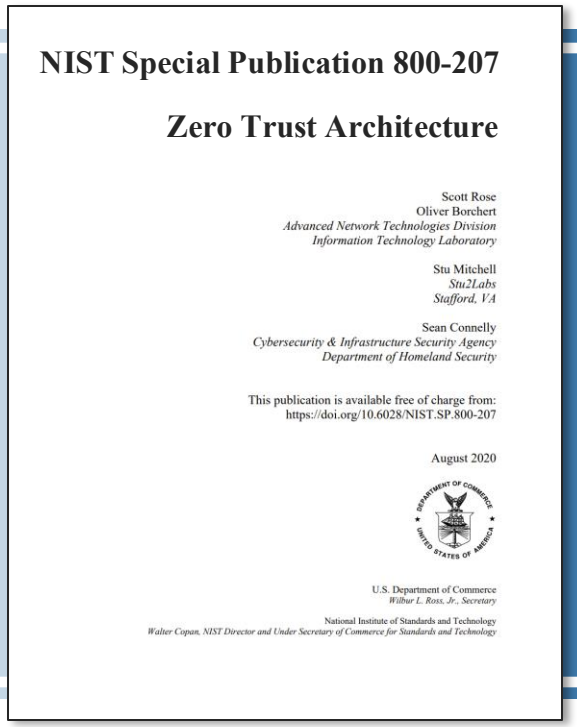
MISSION & VISION

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges

www.nccoe.nist.gov

NCCoE ZTA Demonstration Project

"Implementing a Zero Trust Architecture"



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Advanced Network Technologies Division
Information Technology Laboratory

Stu Mitchell
Stu2Labs
Stafford, VA

Sean Connelly
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

August 2020

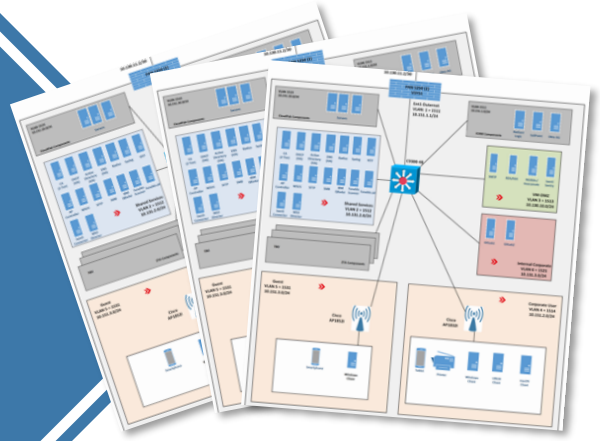
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST SP 800-207, ZTA

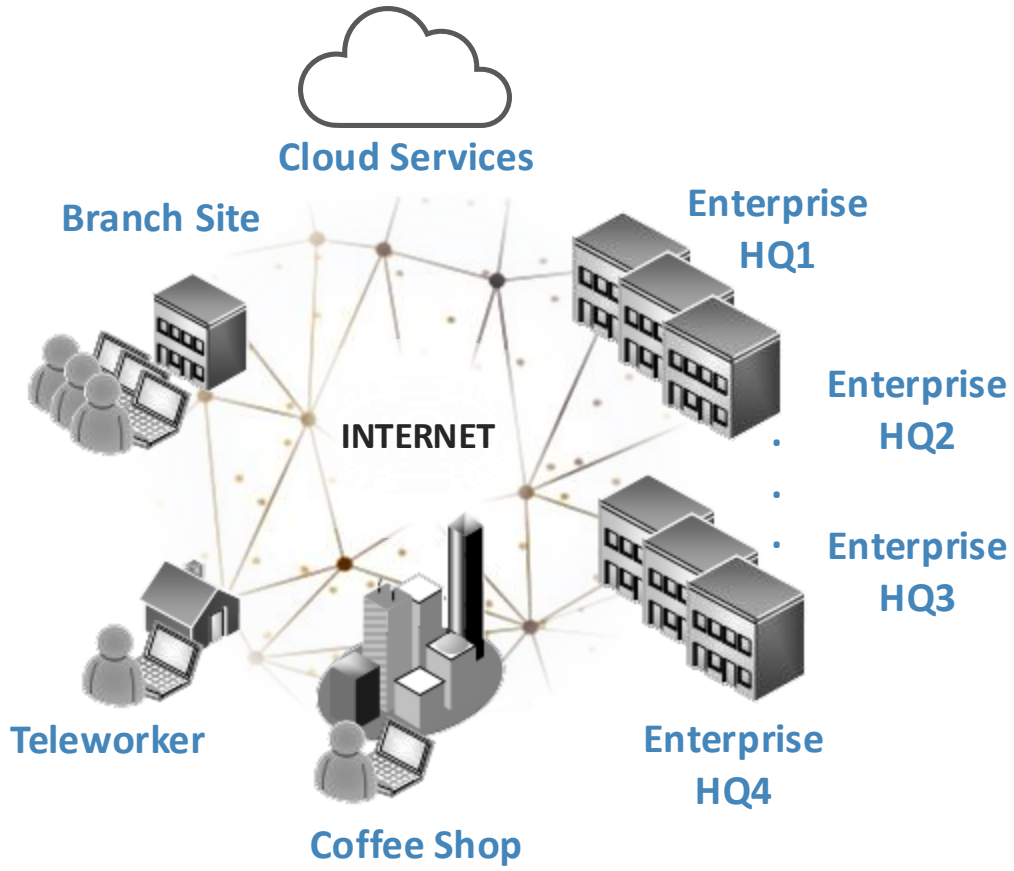
Zero Trust Architecture Deployment Approaches

- Enhanced Identity Governance (EIG)
- Micro-segmentation
- Software Defined Perimeter (SDP)
- Secure Access Service Edge (SASE)



Built 19 Example ZTAs
NIST SP 1800-35

NCCoE ZTA Demonstration Project



NCCoE ZTA Demonstration Project Goals and Focus

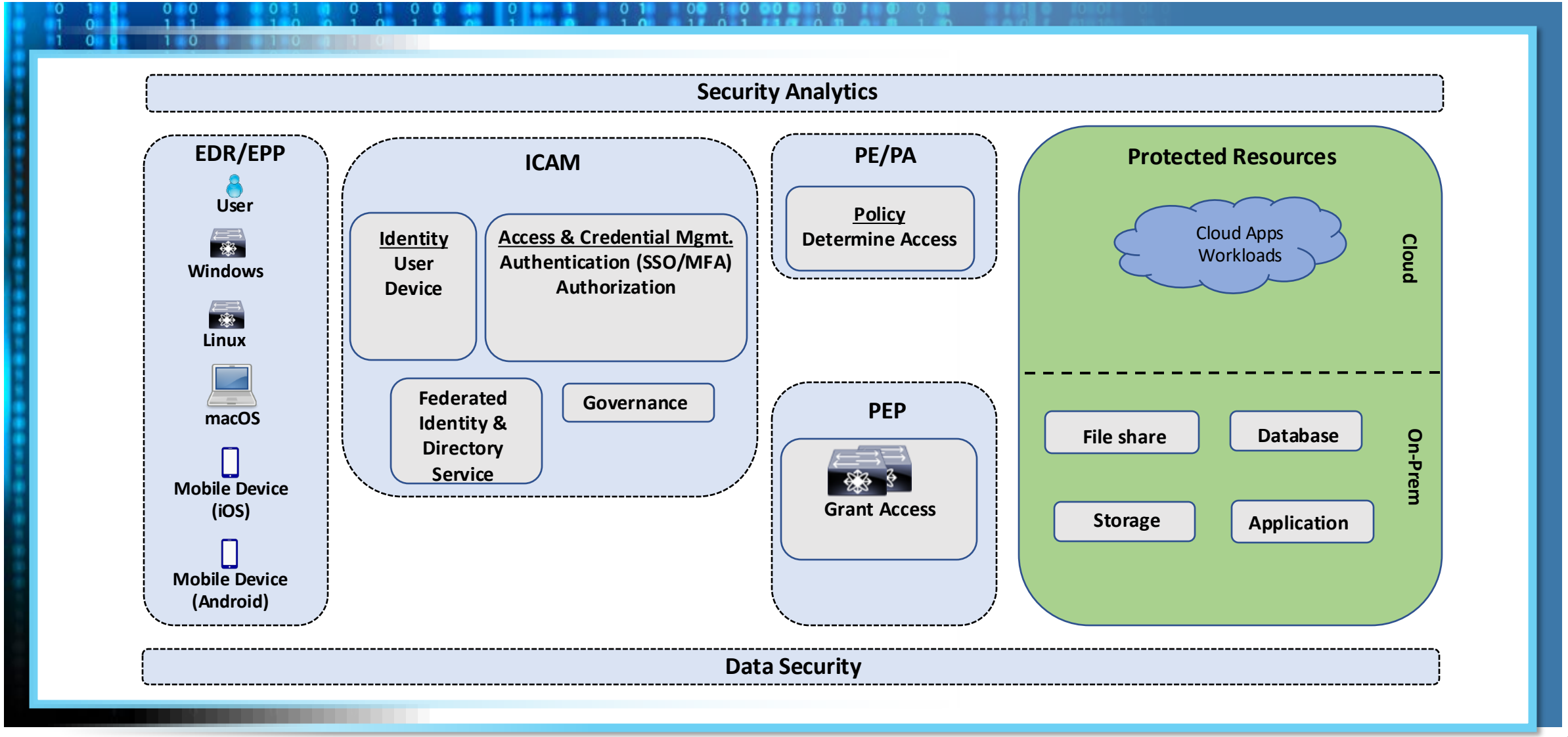
Deployment Approaches

- Enhanced Identity Governance (EIG)
- Micro-segmentation
- Software Defined Perimeter (SDP)
- Secure Access Service Edge (SASE)

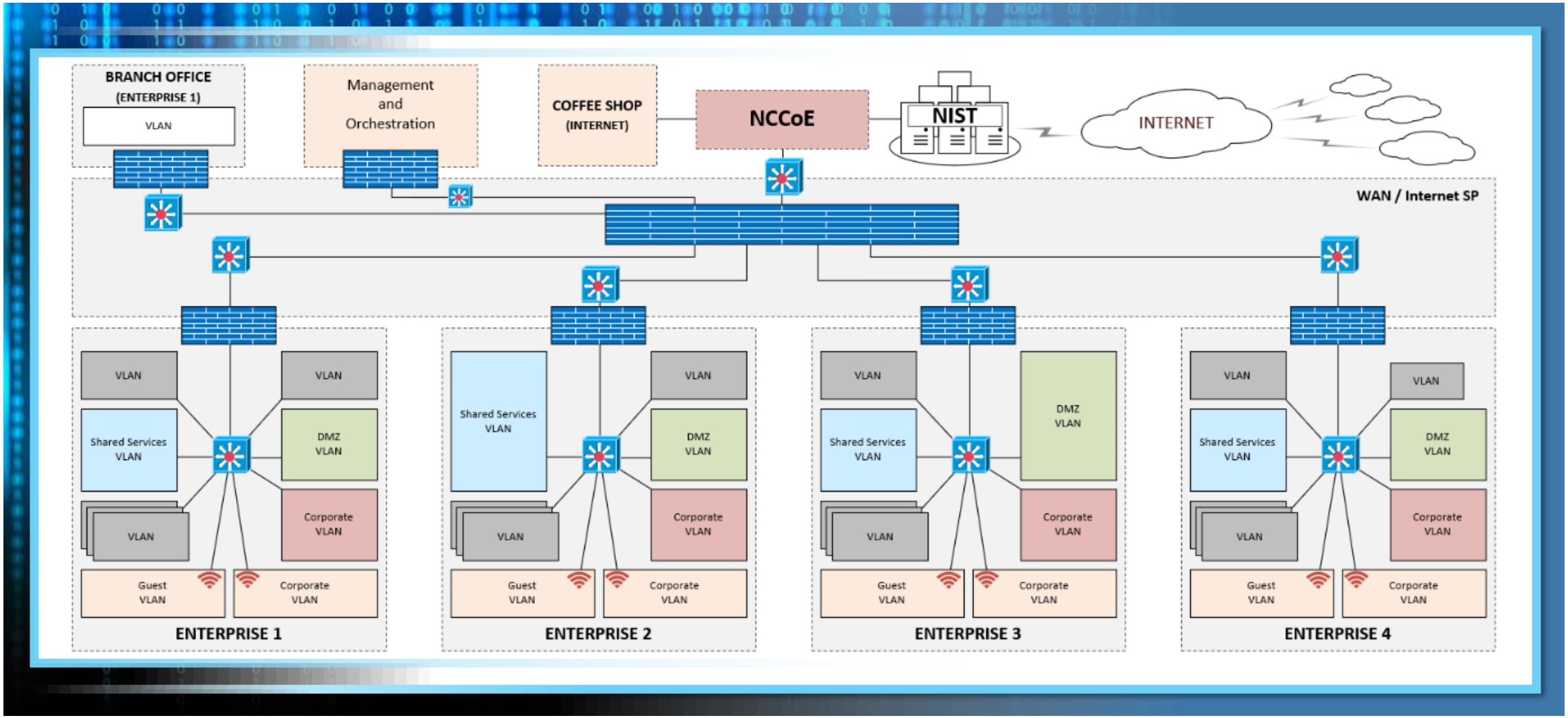
Demonstration Scenarios

- Employee and Contractor Access to Corporate and Internet Resources
- Inter-server Communication
- Cross Enterprise Collaboration
- Trust Score/Confidence Level
- Data Level Security

NCCoE ZTA Reference Architecture



Physical Architecture



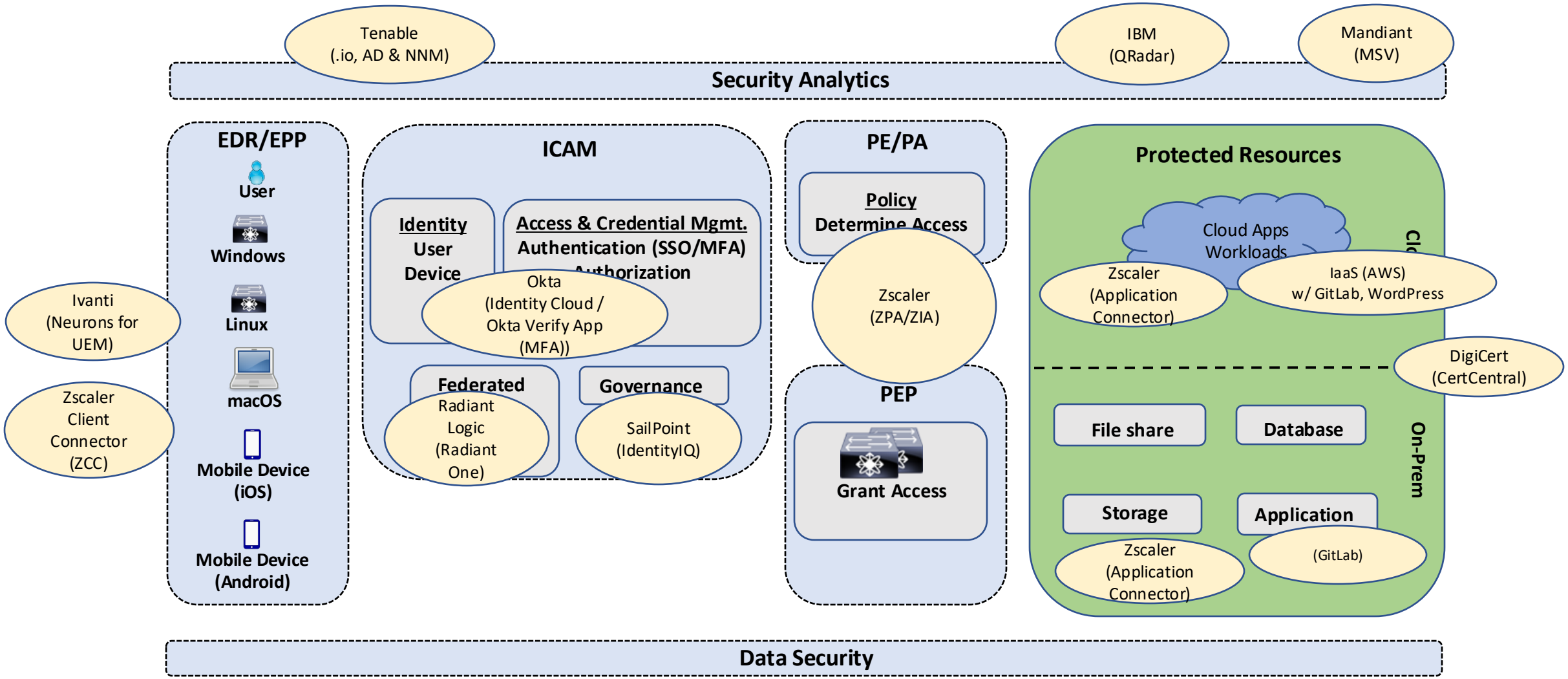
ZTA Collaborating Organizations

- Appgate
- AWS
- Broadcom (Symantec & VMware products)
- Cisco
- DigiCert
- F5
- Forescout
- Google Cloud
- IBM
- Ivanti
- Lookout
- Mandiant
- Microsoft
- Okta
- Omnissa
- Palo Alto Networks
- PC Matic
- Ping Identity
- Radiant Logic
- SailPoint
- Tenable
- Trellix
- Zimperium
- Zscaler

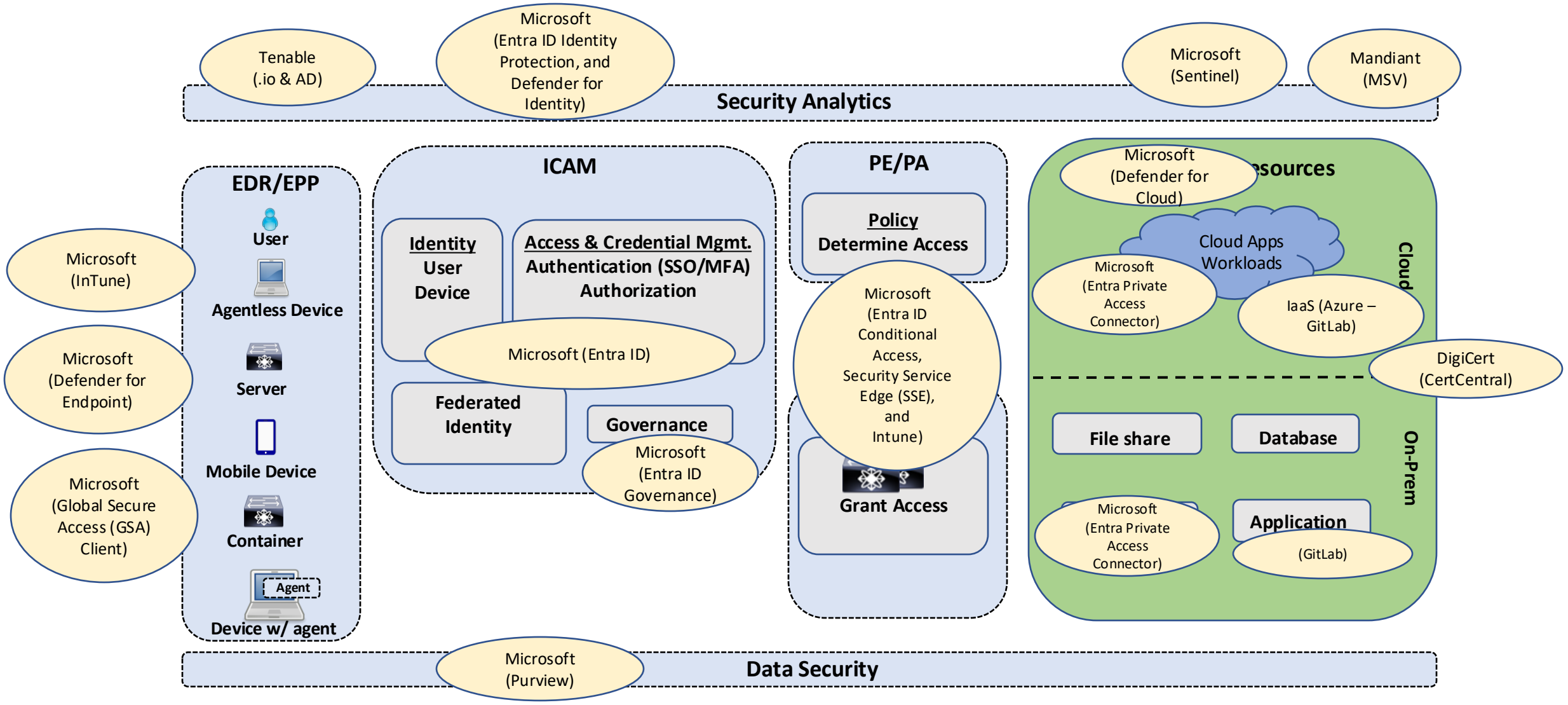
Sample Implementations

**(For details, please refer to *NIST SP 1800-35*
implemented 19 builds, only twp samples are shown here)**

Zscaler as PE



Microsoft as PE



Project Output

NIST SP 1800-35 - June 2025


NIST SPECIAL PUBLICATION 1800-35

Implementing a Zero Trust Architecture:
High-Level Document

Oliver Borchert, Gema Howell, Alper Kerman, Scott Rose, Murugiah Souppaya (National Institute of Standards and Technology); Jason Ajmo, Yemi Fashina, Parisa Grayeli, Joseph Hunt, Jason Hurlburt, Nedu Irrechukwu, Joshua Klosterman, Oksana Slivina, Susan Symington, Allen Tan (The MITRE Corporation); Karen Scarfone (Scarfone Cybersecurity); William Barker (Dakota Consulting); Peter Gallagher, Aaron Palermo (Appgate); Madhu Balaji, Adam Cerini, Rajarshi Das (AWS (Amazon Web Services)); Jacob Barosin, Kyle Black, Scott Gordon, Jerry Haskins, Keith Luck, Dale McKay, Sunjeet Randhawa (Broadcom); Brian Butler, Mike Delaguardia, Matthew Hyatt, Randy Martin, Peter Romness (Cisco); Corey Bonnell, Dean Coclin (DigiCert); Ryan Johnson, Dung Lam, Darwin Tolbert (F5); Tim Jones, Tom May (Forescout); Christopher Altman, Alex Bauer, Marco Genovese (Google Cloud); Andrew Campagna, John Dombroski, Adam Frank, Nalini Kannan, Priti Patil, Harmeet Singh, Mike Spisak, Krishna Yellepeddy (IBM); Nicholas Herrmann, Corey Lund, Farhan Saifudin (Ivanti); Madhu Dodda, Tim LeMaster (Lookout); Ken Durbin, James Elliott, Earl Matthews, David Pricer (Mandiant); Joey Cruz, Tarek Dawoud, Carmichael Patton, Alex Pavlovsky, Brandon Stephenson, Clay Taylor (Microsoft); Bob Lyons, Vinu Panicker (Okta); Peter Bjork, Hans Droishagen (Omnissa); Imran Bashir, Ali Haider, Nishit Kothari, Sean Morgan, Seetal Patel, Norman Wong (Palo Alto Networks); Zack Austin, Shawn Higgins, Rob Woodworth (PC Matic); Mitchell Lewars, Bryan Rossnsteel (Ping Identity); Don Coltrain, Wade Ellery, Deborah McGinn (Radiant Logic); Frank Briguglio, Ryan Tighe (SailPoint); Chris Jensen, Joshua Moll (Tenable); Jason White (Trellix, Public Sector); Joe Brown, Gary Bradt (Zimperium); Jeffrey Adorno, Syed Ali, Bob Smith (Zscaler)

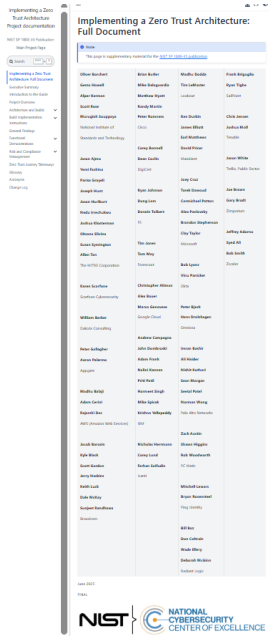
June 2025

FINAL

This publication is available free of charge from https://doi.org/10.6028/NIST.SP.1800-35

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

High Level Document


Implementing a Zero Trust Architecture:
Full Document

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Full Document in Web Format

- Executive Summary, Introduction, & Project Overview
- Architecture and Builds
- Build Implementation Instructions
- Findings
- Functional Demonstrations
- Risk & Compliance Management
- Zero Trust Journey Takeaways

Other Project using Zero Trust

- Leveraging the ZT enterprise environment to support NCCoE's:
  - DevSecOps Practices project

DevSecOps Practices

OBJECTIVE:

Demonstrate and document practical approach and recommendations for DevSecOps practices consistent with NIST Secure Software Development Framework (SSDF)

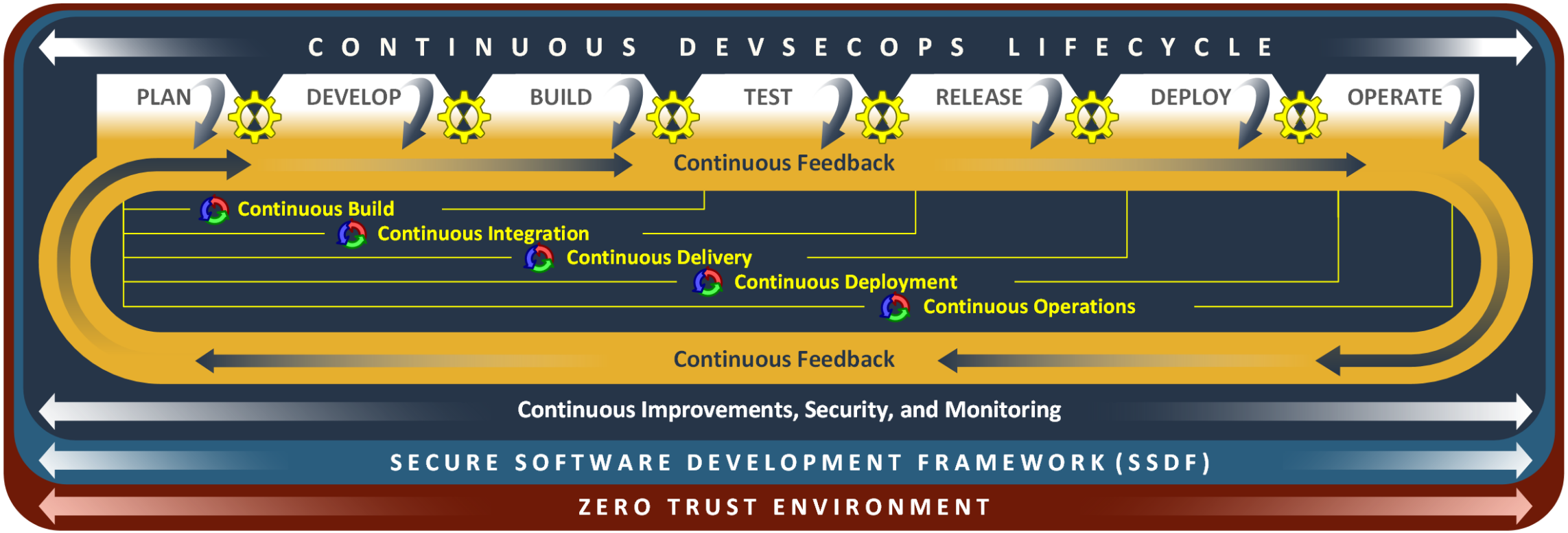
SCENARIOS:

Demonstrate DevSecOps practices in multiple proof-of-concept use case scenarios that involve software development environments integrated with different industry technologies, **including security practices associated with the use of AI capabilities and zero trust architectures**.

- **Closed Source Software Development (initial focus)**
- **Free and Open Source Software (FOSS) Development**

***This project initiated in March 2025 to support the directive outlined in **Section 2(c)(i) of Executive Order 14306**

NCCoE DevSecOps Reference Model



Control Gates

DevSecOps Phases

CI/CD Pipeline

Continues Feedback

Continuous Improvements, Security and Monitoring

Secure Software Development Framework (SSDF)

Overall Security Environment (ZTA)

References

- **ZTA Project Website**

https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

- **DevSecOps Website**

https://www.nccoe.nist.gov/projects/secure-software-development-security-and-operations-devsecops-practices

Questions?

Thank You!

For more information, please contact:

Alper Kerman
Principal Lead for Zero Trust Program
NIST
alper.kerman@nist.gov

Dr. Parisa Grayeli
Principal Cybersecurity Engineer
The MITRE Corporation
pgrayeli@mitre.org and
parisa.grayeli@nist.gov

2026 SSC CYBER EXPO

Zero Trust Self Evaluation for Mission Systems

Mr. Nedu Irrechukwu
Lead Cyber Security Engineer
The MITRE Corporation

Cyber Readiness at the Speed of Space

Agenda

- Introduction
- Motivation
- ZT Gap Analysis
- Self-Evaluation Tool
- Self-Evaluation Process
- Takeaways

Introduction

- Zero Trust shifts from perimeter to data-centric defense, reduces the attack surface, promotes least privilege access and limits lateral movement.
- A Zero Trust architecture provides the infrastructure upon which relevant cybersecurity controls necessary to mitigate known threats are applied and integrated
- Recognizing that Zero Trust implementation is a journey, the DoW outlined two ZT maturity levels (Target and Advanced) in an effort to accelerate ZT adoption

Motivation

- The DoW recognized that Zero Trust Implementation has become a necessity for components to adequately protect and mitigate modern threats
- DoW components expected to meet ZT Target Level maturity by September 2027
- The DAF I-Plan outlines a gap analysis as an early step towards the ZT Implementation

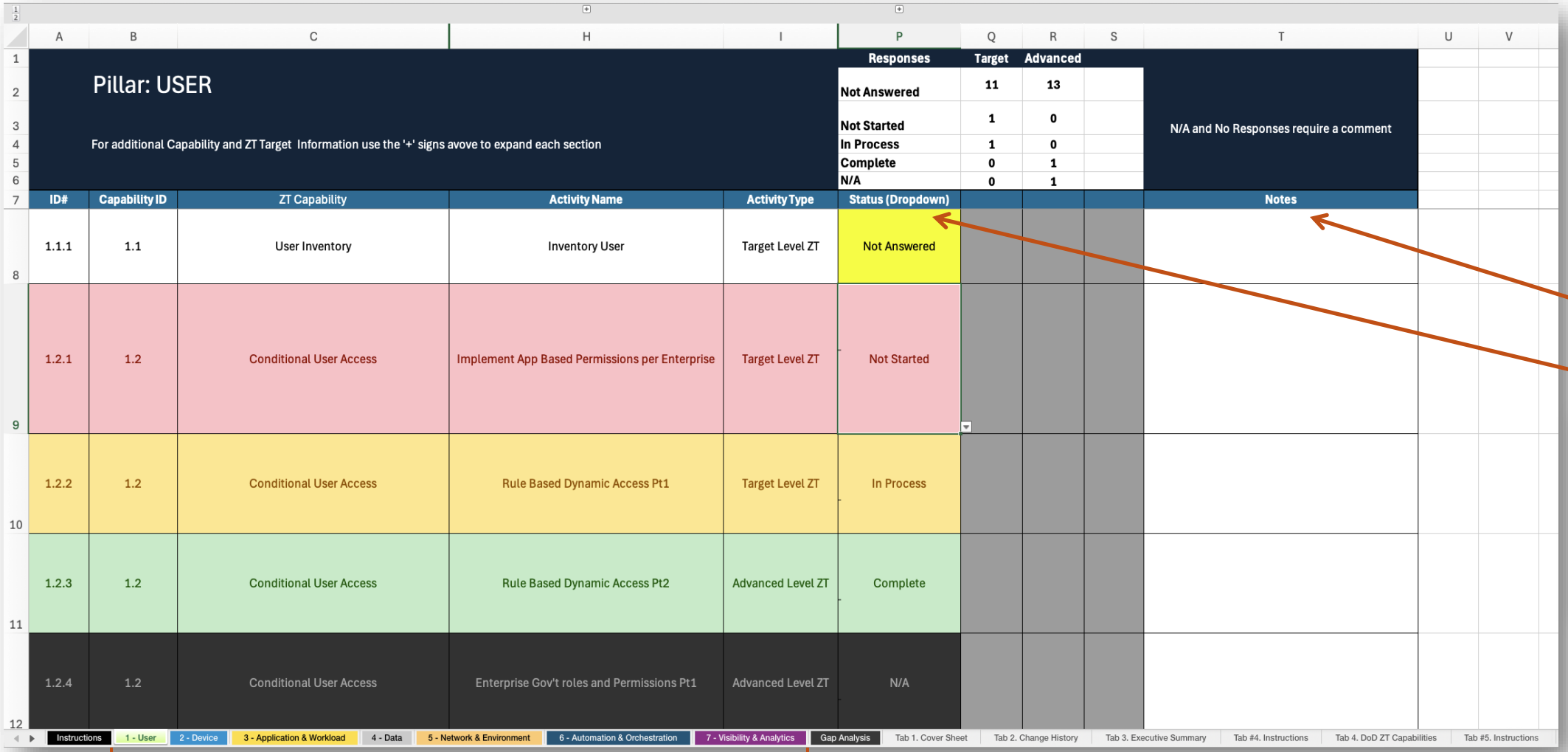
Zero Trust Gap Analysis

- Target encapsulates the minimum set of capability outcomes and activities that necessary to mitigate against currently known threats
- There are 91 Activities in Target level maturity and 61 in Advanced level maturity
- Using S6's spreadsheet self-evaluation tool, the assessment process evaluates existing controls and processes against Target level maturity
- SSC/S6 proactively engaging with mission systems to help conduct a gap analysis via the ZT self assessment process

Self Evaluation Tool

- Tool facilitates the process of evaluating ZT maturity based on DoW ZT Activities
- Tool represents the Target and Advanced Level Activities by Pillar
- Each tab or worksheet represents a pillar, each row represents an Activity
- Gap Analysis tab provides a high-level view of results including results per pillar

Self-Evaluation Tool - Responses



Pillar: USER

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

Responses	Target	Advanced
Not Answered	11	13
Not Started	1	0
In Process	1	0
Complete	0	1
N/A	0	1

N/A and No Responses require a comment

ID#	Capability ID	ZT Capability	Activity Name	Activity Type	Status (Dropdown)	Notes
1.1.1	1.1	User Inventory	Inventory User	Target Level ZT	Not Answered	
1.2.1	1.2	Conditional User Access	Implement App Based Permissions per Enterprise	Target Level ZT	Not Started	
1.2.2	1.2	Conditional User Access	Rule Based Dynamic Access Pt1	Target Level ZT	In Process	
1.2.3	1.2	Conditional User Access	Rule Based Dynamic Access Pt2	Advanced Level ZT	Complete	
1.2.4	1.2	Conditional User Access	Enterprise Gov't roles and Permissions Pt1	Advanced Level ZT	N/A	

Instructions | 1 - User | 2 - Device | 3 - Application & Workload | 4 - Data | 5 - Network & Environment | 6 - Automation & Orchestration | 7 - Visibility & Analytics | Gap Analysis | Tab 1. Cover Sheet | Tab 2. Change History | Tab 3. Executive Summary | Tab #4. Instructions | Tab 4. DoD ZT Capabilities | Tab #5. Instructions

Notes

Status

Responses
Not Answered
Not Started
In Progress
Complete
N/A

ZT Pillars

Self-Evaluation Tool

Description

Outcomes

End State

Responses
Not Answered
Not Started
In Process
Complete
N/A

Descriptions	Outcomes	End State	Predecessor(s)	Successor(s)	Status (Dropdown)
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.* *2. Identified managed privileged users.* *3. Identified applications using their own user account management for non-administrative and administrative accounts.* *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*	Not Answered
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.* *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.* *3. Components identify attributes associated with PAM activities within their environment.* *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.*			Not Started
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.* *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*	In Process
DoD Components expand the development of rules for dynamic access decision making accounting for risk. Solutions used for dynamic access are integrated with cross pillar Machine Learning (ML) and Artificial Intelligence (AI) functionality enabling automated rule management.	1. Components and services are fully utilizing rules to enable dynamic access to applications and services. 2. Technology utilized for Rule-Based Dynamic Access supports integration with AI/ML tooling.	None identified in DoD Documentation	Rule Based Dynamic Access Pt1; File Activity Monitoring Pt2	None identified in DoD Documentation	Complete

Self-Evaluation Tool

** 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.

Target Level Gap Analysis Matrix

Pillar	Not Answered	Not Started	In Process	Complete	N/A	Target Total	Target Level Completion	Target At Risk	Target Not
User	4	3	3	1	2	13	9%	10	2
Devices	14	0	0	0	0	14	0%	14	0
Application & Workload	12	0	0	0	0	12	0%	12	0
Data	17	0	0	0	0	17	0%	17	0
Network & Environment	10	0	0	0	0	10	0%	10	0
Automation & Orchestration	13	0	0	0	0	13	0%	13	0
Visibility & Analytics	12	0	0	0	0	12	0%	12	0
Total	82	3	3	1	2	91	1%	88	2

Advanced Level Gap Analysis Matrix

Pillar	Not Answered	Not Started	In Process	Complete	N/A	Advanced Total	Advanced Level Completion	Advanced At Risk	Advanced Not
User	2	3	3	4	3	15	33%	8	3
Devices	10	0	0	0	0	10	0%	10	0
Application & Workload	6	0	0	0	0	6	0%	6	0
Data	14	0	0	0	0	14	0%	14	0
Network & Environment	3	0	0	0	0	3	0%	3	0
Automation & Orchestration	7	0	0	0	0	7	0%	7	0
Visibility & Analytics	6	0	0	0	0	6	0%	6	0
Total	48	3	3	4	3	61	7%	54	3

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	
Complete	Target Level activities that have been fully implemented	
N/A	Activities the Component assesses are not applicable to the entire	*Requires a comment in the annex
Target Total	Total Number of Activities	
Target/Advanced 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
Target/Advanced 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	*Requires a comment in the annex
Target/Advanced 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.

SSC/S6 Version: 1.1

Date of Last Update: 10 March 2026

Instructions | 1 - User | 2 - Device | 3 - Application & Workload | 4 - Data | 5 - Network & Environment | 6 - Automation & Orchestration | 7 - Visibility & Analytics | Gap Analysis | Tab 1. Cover Sheet | Tab 2. Change History

Gap Analysis Worksheet

Self Evaluation Process

- **Discussion-Based**
  - Each Activity in each pillar is discussed with the mission systems' verbal input as our primary data source
- **ZT Outcome Clarification**
  - Assessment team speaks to the intent of each ZT activity and provides clarification as needed
- **Consensus Scoring**
  - Team selects responses in the assessment template based on group agreement
- **Data Capture**
  - Results and metrics are captured in the ZT self-assessment spreadsheet. System configuration details are usually not captured in the Spreadsheet to keep it unclassified. System owners can add classified notes their own copy of the tool after the assessment

Takeaways

Mission Systems are finding it challenging to:

Define/Select an architecture approach to implement ZT (NIST SP 800-207 and 1800-35 suggests the following approaches EIG, SDP, SASE, Microsegmentation etc.)

Identify the ZT architecture components, solutions, and integrations required to implement Zero Trust environment

Outline structured/prioritized steps that provide a guided pathway to achieving Target level maturity

Conclusion

- The self-assessment process identifies ZT gaps existing in the environment and serves as an important milestone in the ZT journey

- Mission Systems need a phased approach for ZT adoption and a ZT Solution/Vendor framework to help remediate gaps

- SSC stands ready to assist

Questions?

2026 SSC CYBER EXPO

Zero Trust Assessment Vendor Framework

Dr. Safwa Ameer
Applied Cyber Security Engineering, Lead
The MITRE Corporation

Cyber Readiness at the Speed of Space

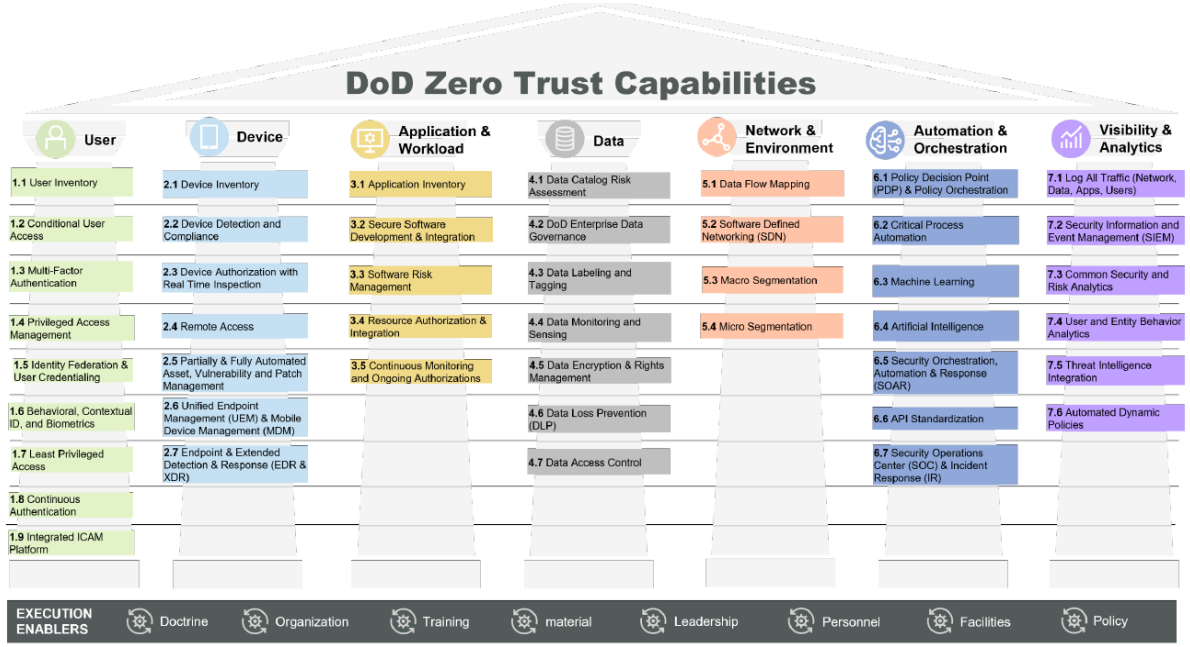
Agenda

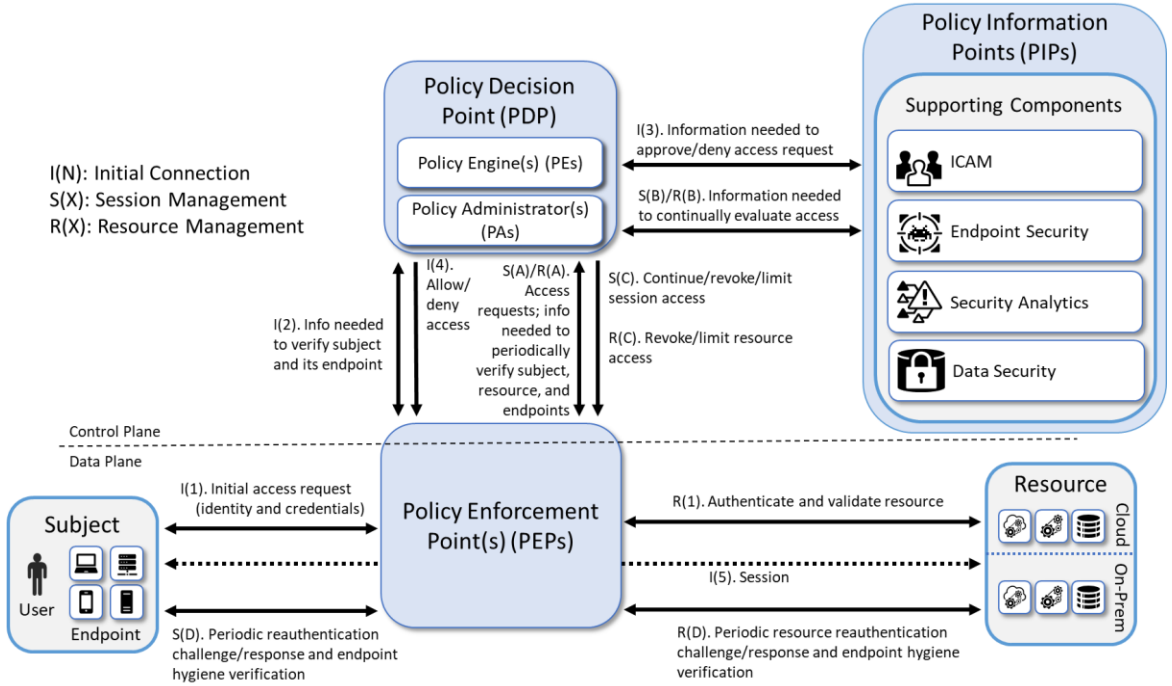
- Motivation
- Approach
- ZTA vendor framework
- Structured Approach Toward Addressing DOW ZT Activities
- Conclusion

Motivation

To support the mission systems program in selecting ZT commercial solutions that align with the DOW ZT framework and NIST ZT guidelines

Approach





We performed a comprehensive mapping between the NIST ZTA components categories* and the DOW ZT Activities.

* NIST SP 800-207 Zero Trust Architecture, August 2020

ZT Vendor Framework

PDP

Endpoint Security

1. Endpoint Detection and Response (EDR)/Endpoint Protection Platform (EPP)
2. Unified Endpoint management (UEM)/mobile Device management (MDM)
3. Continuous diagnostics and mitigation (CDM)

PEP

Data Security

1. Data discovery
2. Data classification, labeling, and sanitization
3. Data encryption
4. Data integrity
5. Data availability
6. Data access protection and exfiltration

ICAM

1. Identity management
2. Access and credential management
3. Multi-factor authentication
4. Identity governance
5. Federated identity

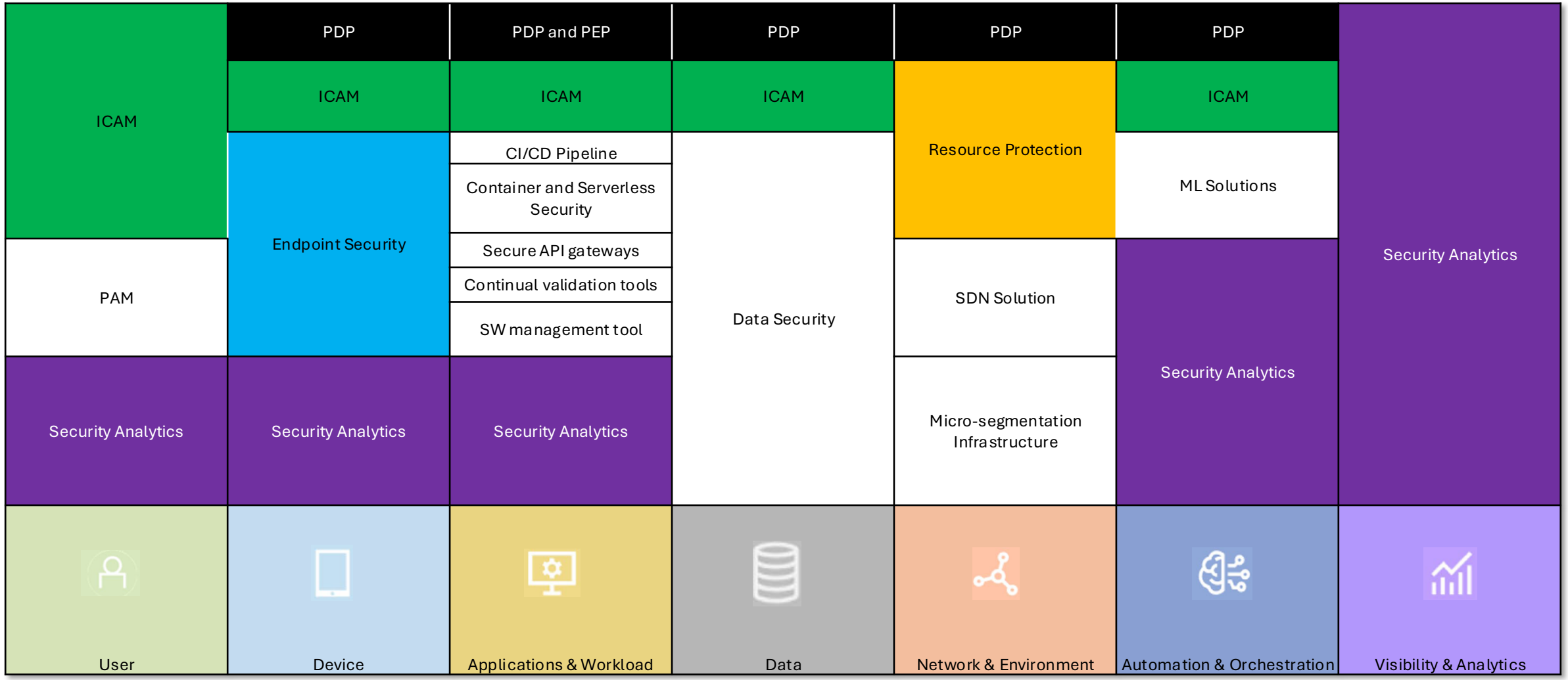
Resource Protection

1. Application connector
2. Cloud workload protection
3. Cloud security posture management

Security Analytics

1. SIEM
2. SOAR
3. Vulnerability scanning and assessment
4. Network discovery
5. Security controls validation
6. Identity monitoring
7. Security monitoring
8. Application protection and response
9. Cloud access permission manager
10. Security analytics and access monitoring
11. Network monitoring
12. Traffic inspection
13. Endpoint monitoring
14. Threat intelligence
15. User behavior analytics
16. Firmware assurance
17. Centralized management

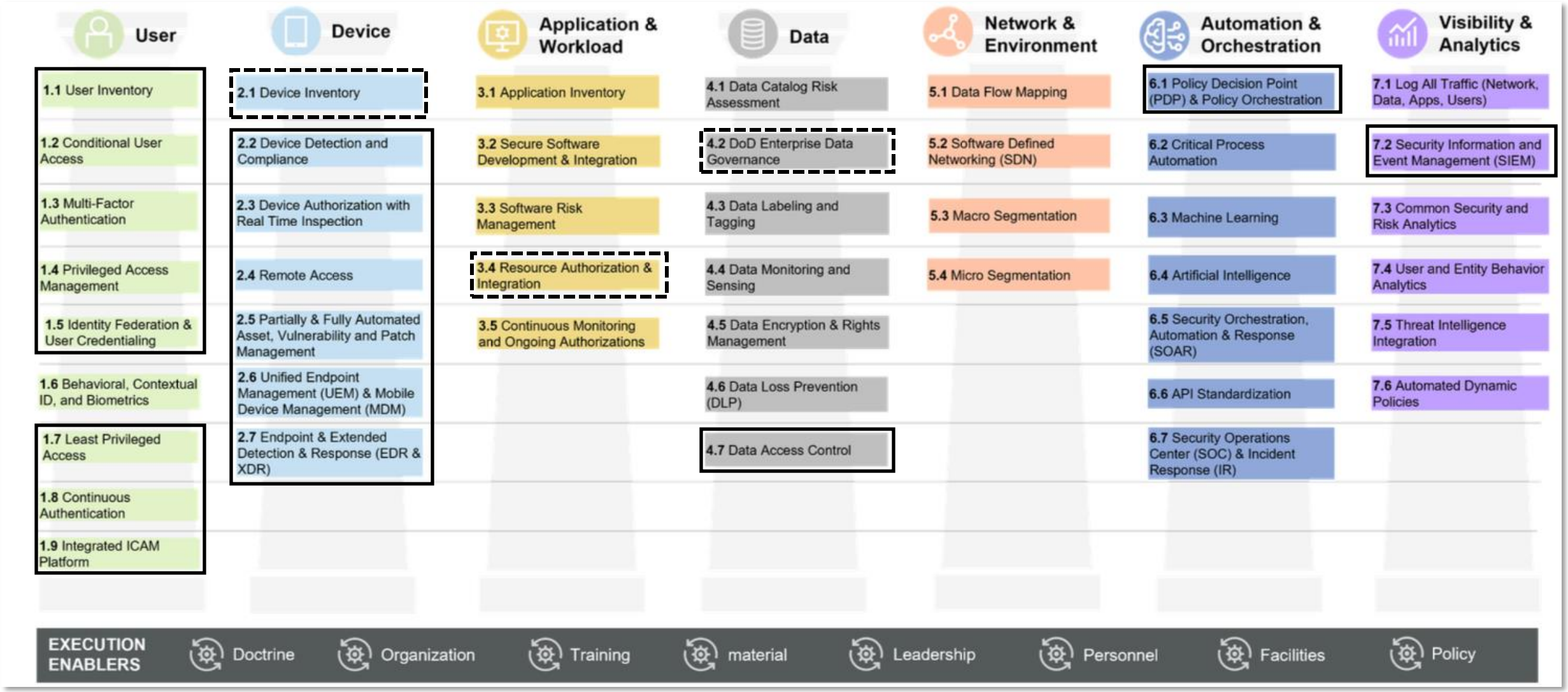
Solution Categories Coverage



Structured Approach Toward Addressing DOW ZT Activities

- NIST ZTA approaches
  - Phase 1: EIG Crawl Reference Architecture
  - Phase 2: EIG Run Reference Architecture
  - Phase 3: ZTA Using Software Defined Perimeter (SDP) , ZTA Using Micro-Segmentation, and ZTA Using SASE approaches
- For each ZTA approach, we identified the DoW ZT activities it supports, and the solution categories required to enforce them

Minimum Activities Required to Achieve ZTA



Conclusion

- SSC/S6 stands ready to assist in selecting Zero Trust solutions that support DOW Zero Trust target-level activities and align with NIST Zero Trust guidelines.

Questions?

Thank You!

For more information, please contact:

Dr. Safwa Ameer
Applied Cybersecurity Engineering, Lead
saameer@mitre.org

Nedu Irrechukwu
Lead Cyber Security Engineer
cirrechukwu@mitre.org

2026 SSC CYBER EXPO

Zero Trust Defense in Satellites

Building Cyber-Secure Satellites

Mr. Nicholas Cohen
Principal Engineer
The Aerospace Corporation

Cyber Readiness at the Speed of Space

The Challenge: Satellites aren't IT Systems

Typical IT System

- User Access Control
- Easy to Upgrade
- Unlimited Power/Bandwidth
- Always Connected
- Full Traffic Logging

Satellite Systems

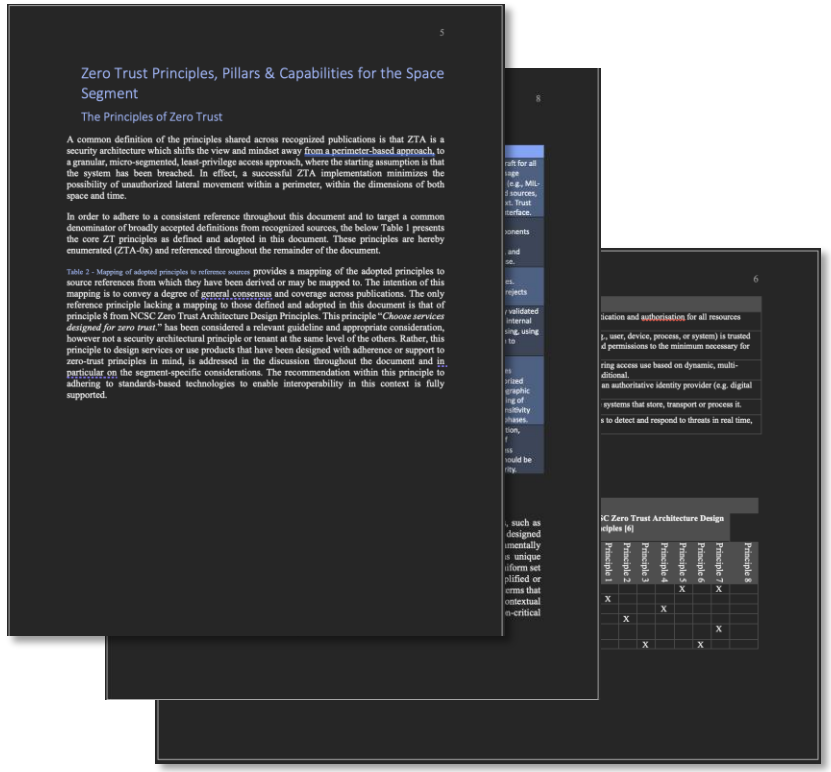
- No traditional "Users" or User-Based Access Control
- Inaccessible or unaffordable for upgrades after design phase
- Resource Limited – Power, Bandwidth, Memory
- Intermittent Connectivity
- Limited Loggin due to resource constraints

Standard Zero Trust guidance doesn't work for satellites

Solution: SV Specific ZT Implementation Guidance

SSC/S6 and SSIO is creating an SV Cybersecurity Reference Architecture that will:

- Provide practical implementation guidance for SV design
- Save programs time and effort when implementing zero trust
- Aligned with DoD Zero Trust Reference Architecture, NIST 800-207 Zero Trust Pillars, and RMF requirements
  - Identity, Devices, Network, Applications & Workloads, Supporting
  - Tailored to space systems
- Contain Reference Desing for payload, bus, communications
- Designed in collaboration with ESA, Department of Homeland Security



Align space system zero trust with existing guidance

Road: Principles to Implementation

ZT Principles

- Verify access independent of location and perimeter
- Limit trust of all resources based on least privilege
- Enforce continuous and dynamic verification
- Authenticate all resources with verifiable and managed identity
- Data-centric security
- Audit and log all events and leverage monitoring analytics

ID	Mapped Reference Tenets and Principles																										
	Department of Defense (DoD) Zero Trust Reference Architecture [4]												NIST Special Publication 800-207 - Zero Trust Architecture [2]							NCSC Zero Trust Architecture Design Principles [6]								
	Tenet 1	Tenet 2	Tenet 3	Tenet 4	Tenet 5	Principle 1	Principle 2	Principle 3	Principle 4	Principle 5	Principle 6	Principle 7	Tenet 1	Tenet 2	Tenet 3	Tenet 4	Tenet 5	Tenet 6	Tenet 7	Principle 1	Principle 2	Principle 3	Principle 4	Principle 5	Principle 6	Principle 7	Principle 8
ZTP-01	X	X				X		X						X										X		X	
ZTP-02			X										X		X					X							
ZTP-03				X					X			X				X		X					X				
ZTP-04							X														X						
ZTP-05										X				X												X	
ZTP-06					X						X						X		X			X			X		

Zero Trust Principles map to multiple sources of guidance

Capabilities

- Mapped to DoD/CISA Zero Trust Capabilities
- Mapped to SPARTA countermeasures, ensuring capabilities are relevant for spacecraft
- 100% coverage of both DoD capabilities and SPARTA countermeasures relevant to ZT

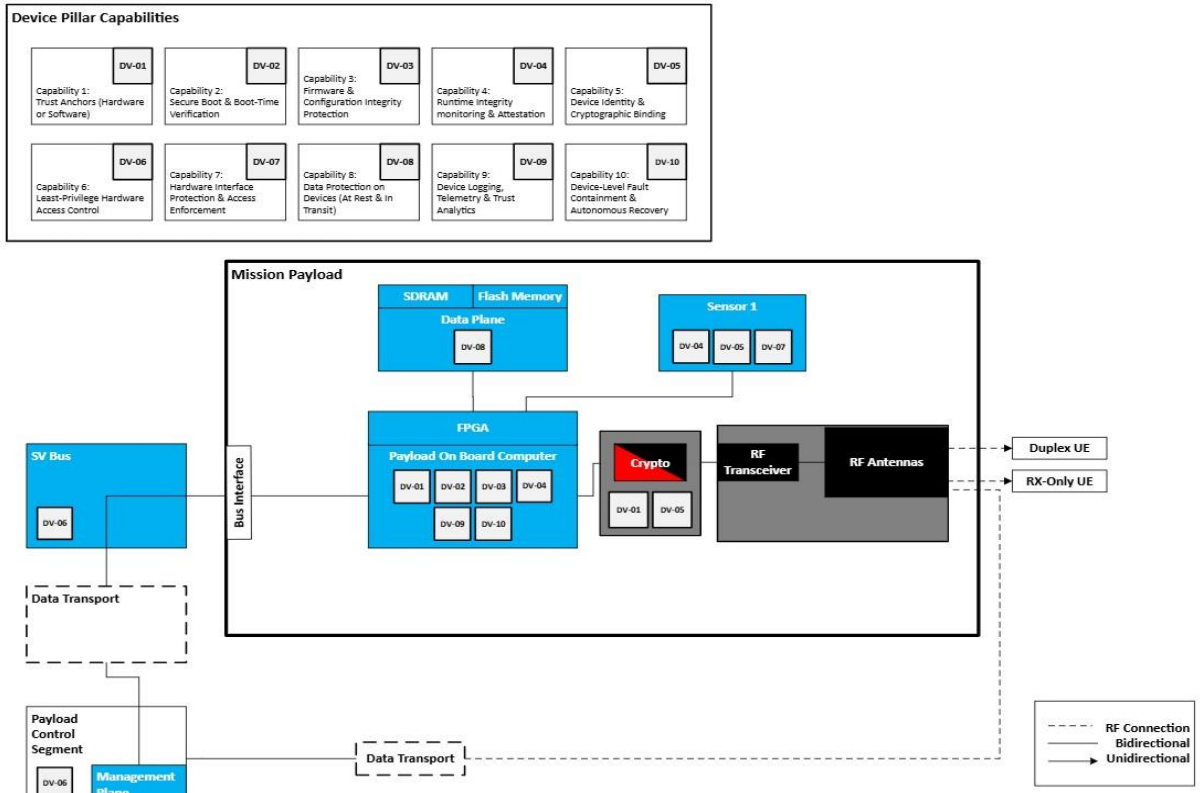
Primary contribution of this project

Implementation

- SSIO's primary contribution is filling in details about how to implement zero trust for spacecraft
- Goal is to provide useful guidance on how to meet the intent of zero trust
- Leaning on subject matter expertise, commercial offerings, and research

Example: Payload Reference Architecture

- Using simplified payload and bus reference designs, we're applying zero trust principles to spacecraft design
- Goal is to create a zero trust guide that fits most cases and can be easily tailored
- Make it easy for programs to adopt zero trust without having to create requirements from scratch

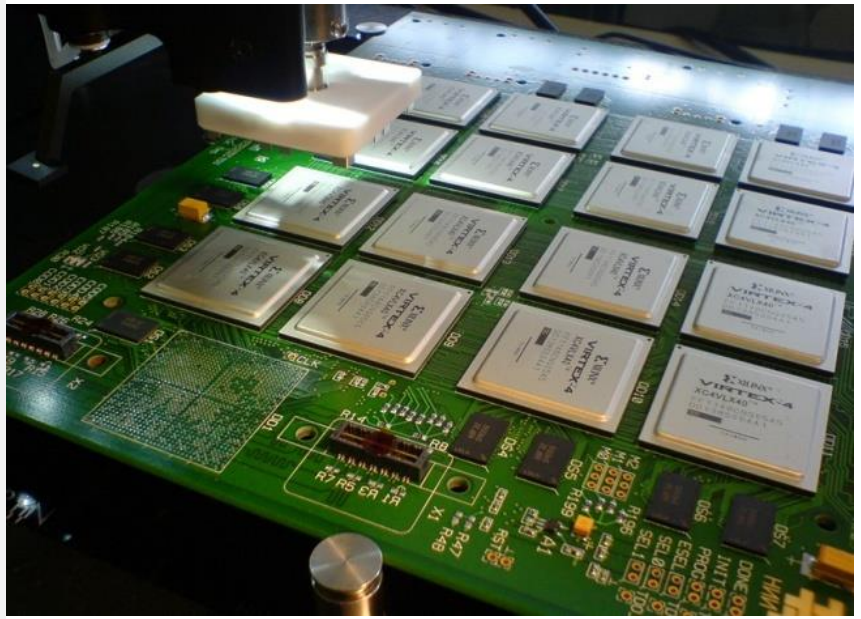


Zero trust capabilities mapped to a reference payload

Make it easy for programs to implement zero trust correctly

Deep Dive: HW Root of Trust

- Enables continuous assurance in firmware and software
  running onboard the vehicle
- Hardware root of trust (trusted platform module, physically unclonable functions)
- Software root of trust (ROM-based bootloader, embedded keys)
- Initial trust anchor provisioning
- Cryptographic key anchoring



Create a strong foundation for zero trust at the device level

Next Steps

- Anticipating draft guidance in June for spacecraft bus
- Add payload, comm references
- Translate to requirements
- Validate implementations in a lab environment
  - Collaboration with OTTI CyDER, MITRE, 6 STS to build representative environments
- Participate with industry: Trusted Computing Group now has a Satellite Working Group!
- Identify and evaluate products and technologies that can implement zero trust
  - AFRL is developing several early technologies including Cyber Hardened Satellite Services

Questions?

Thank You!

For more information, please contact:

Nicholas Cohen
Principal Engineer
nicholas.cohen@aero.org

Wednesday, April 22nd
Dining Options

BX Restaurants
Tenkatori
Gusto's
Coffee & Bakery

Food Trucks
BatterBerries
Gochu Gang KBBQ
Ice cream (Dip Deez)

South Bay Bar & Grill
$15 Buffet Special
Fried or baked chicken
2 Sides & side salad
Dinner Roll & Drink

LUNCH

Visit Show & Tell Room & Exhibitors
See you at 1245!

Cyber Readiness at the Speed of Space

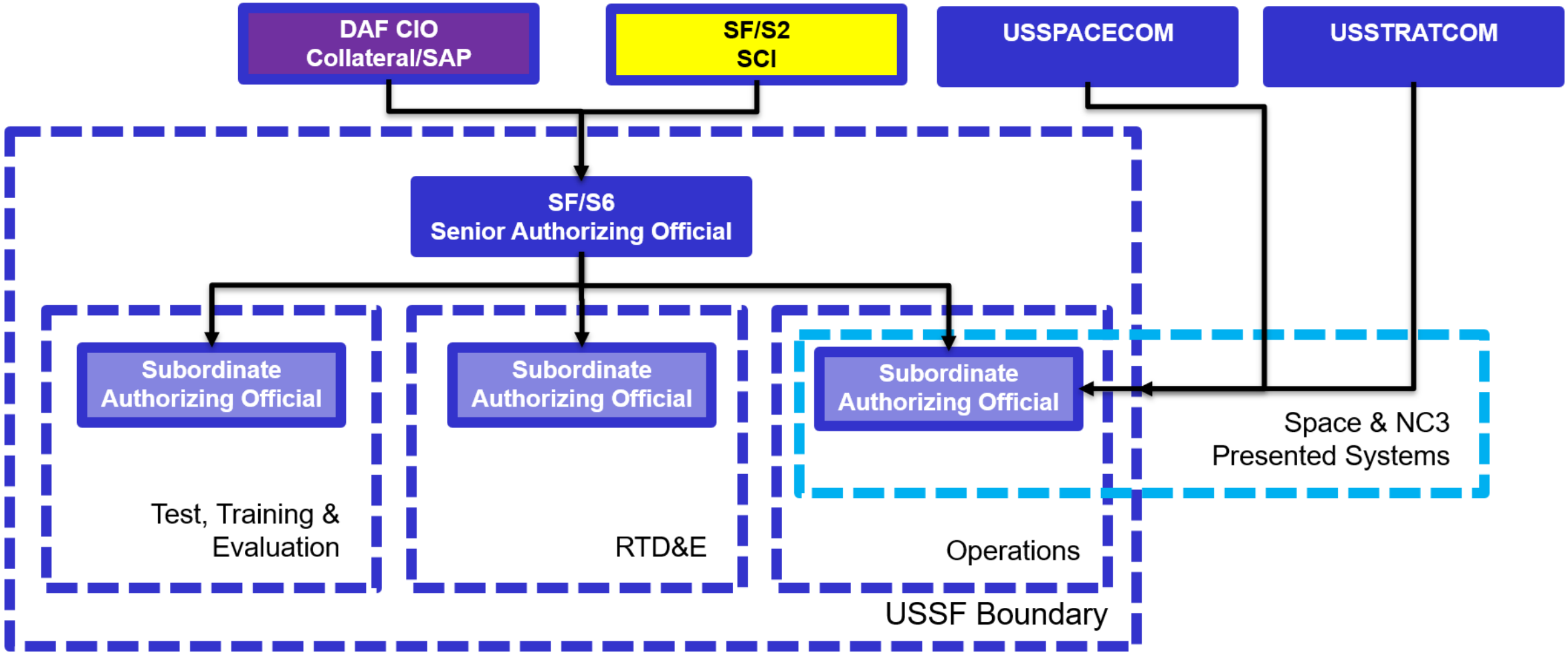
2026 SSC CYBER EXPO

Authority to Operate

Risks, Security Measures, and Processes Explained

Mr. Seth Whitworth
Associate Deputy Chief of Space Ops for Cyber & Data
USSF HQ S6

USSF Boundary



Questions?

2026 SSC CYBER EXPO

Project Enigma Overview

Accelerating Space Acquisition Through Secure Digital Collaboration

Mr. Phil Chen

SSC SYD 88

Cyber Readiness at the Speed of Space

Agenda

- What is Enigma?
- Why Enigma?
- Architecture
- Capabilities
- Tools
- Questions

What is Enigma?

Mission

Provide an IL6 collaborative Digital Engineering Environment (DEE) for the U.S. Space Force, Space Systems Command (SSC), industry and government stakeholders.

Scope

Connects government stakeholders with authorized industry partners.

Purpose

Maintain Authoritative Source of Truth (ASoT) by transforming Classified data collaboration at the speed of relevance to meet acquisition reform.

Model

A Government Owned – Contractor Operated (GOCO) hybrid Platform-as-a-Service (PaaS) solution.

Enigma is transforming how Classified data is collaborated between government and industry

Why Enigma?

No classified multi-enclave collaborative environment between government and industry exists

Traditional data transfer “sneakernet” delays acquisition schedules and introduce major security vulnerabilities

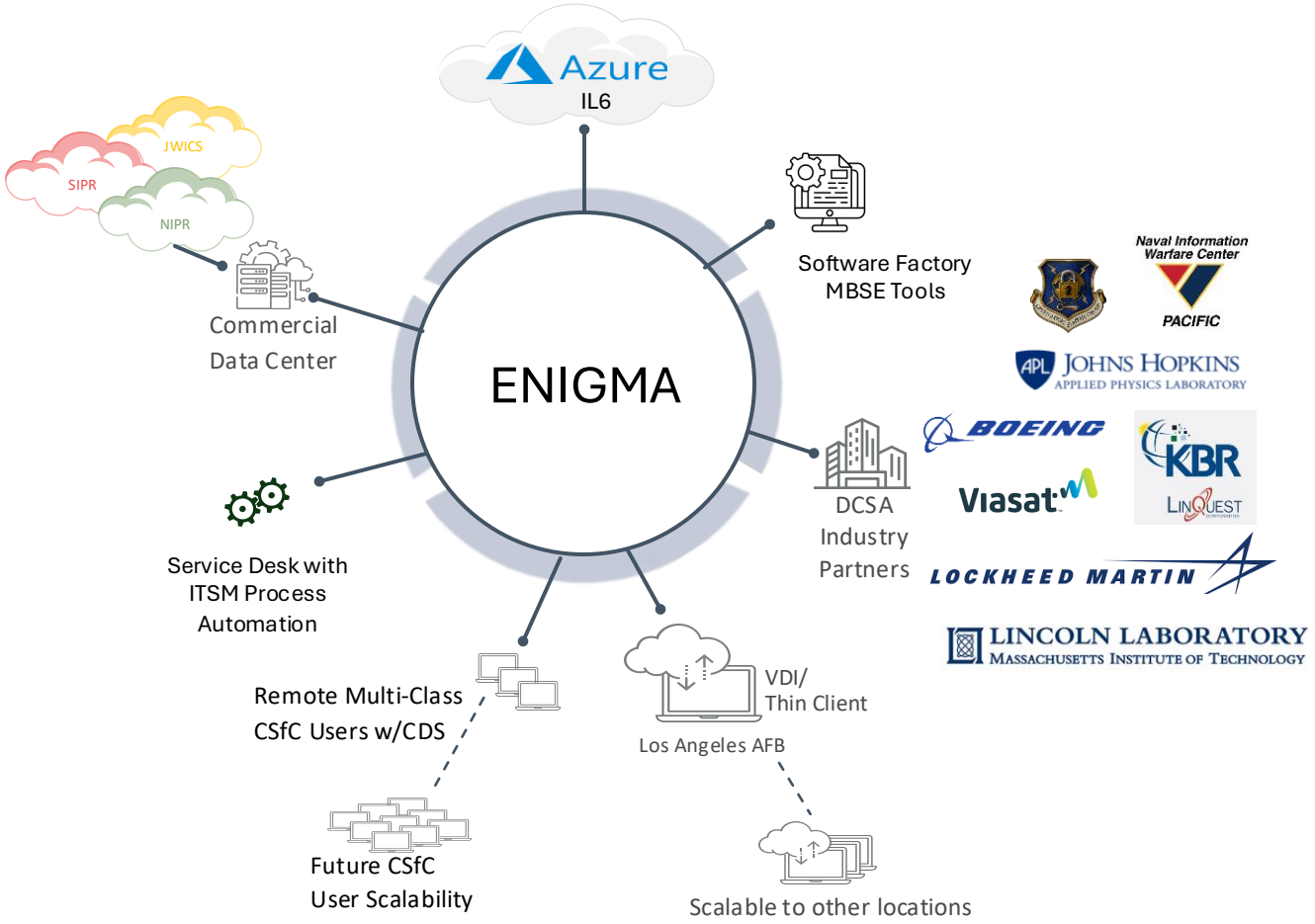
No collaborative Digital Engineering Environment (DEE) at IL6

Legacy systems no longer meet USSF operational, acquisition, and mission needs

Ability to on-board enabling functionality is either prohibited or significantly delayed

Current networks lack remote capabilities, capacity, speed, and physical end-user devices

Architecture



- Software Factory with required MBSE Tools creates baseline for collaboration environment
- Connectivity of Six Industry Partners via Commercial Ethernet Gateway (CEG)
- Government access layer at LAAFB via Citrix VDI Trusted Thin Clients (TTC) with scalable capability
- Commercial Data Center scalable to TS/SCI and SAP

ATO granted at a High-High-High (H-H-H) Confidentiality, Integrity, and Availability

NSA-Approved Commercial Solutions for Classified (CSfC) for secure remote access

Capabilities

Operational Capabilities as of Today

- ✓ H-H-H IL6 ATO
- ✓ Industry partner classified network connections
- ✓ Bi-directional data transfer
- ✓ ICAM, SSO
- ✓ Software onboarding
- ✓ Software Development with Software Factory
- ✓ VDI with SIPR Access
- ✓ Collaboration & Digital Engineering
- ✓ License Management
- ✓ IT Service Management
- ✓ Service Desk Operations

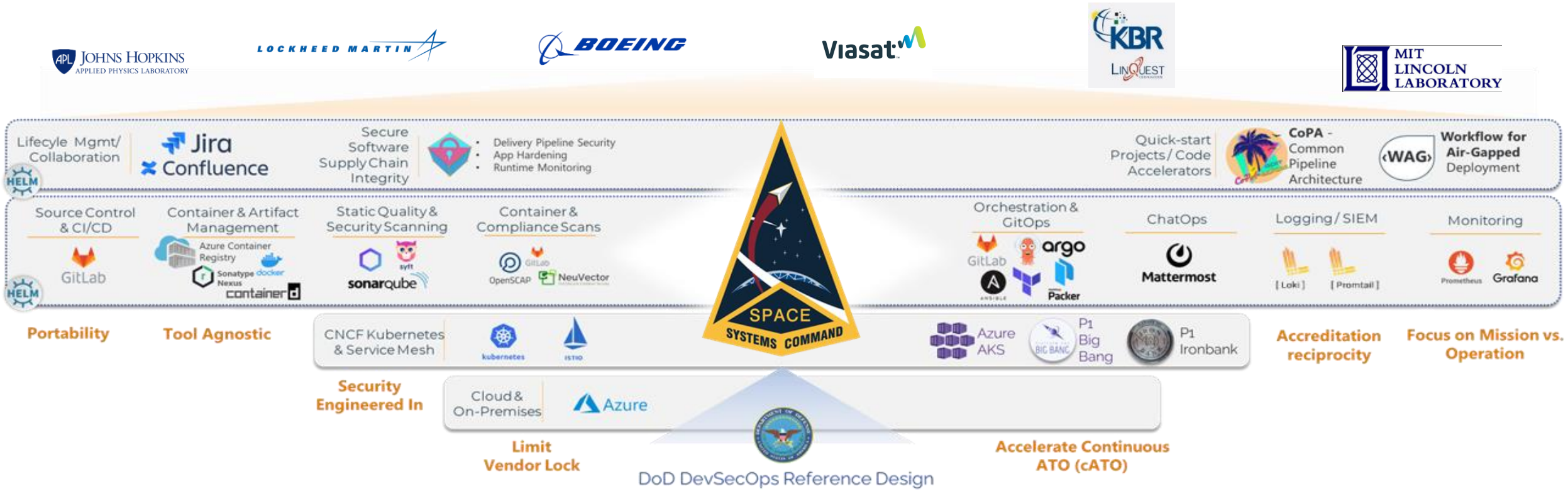
Capabilities in Progress

- ❑ Stakeholder onboarding
- ❑ CSfC Laptop
- ❑ CI/CD pipeline
- ❑ Additional Software (Adobe Acrobat/ACEIT/SSI/OnePager)

Future Capabilities

- ❖ Full Zero Trust
- ❖ Multi-Cloud
- ❖ E-ICAM
- ❖ Post Quantum Cryptography
- ❖ Enable integration with AI capabilities
- ❖ Multiple classification levels (TS, TS SCI, SAP)
- ❖ Digital Twin Hosting

Tools


JOHNS HOPKINS APPLIED PHYSICS LABORATORY
LOCKHEED MARTIN
BOEING
Viasat
KBR
LinQuest
MIT LINCOLN LABORATORY
Lifecyle Mgmt/ Collaboration
Jira
Confluence
Secure Software Supply Chain Integrity
Delivery Pipeline Security
App Hardening
Runtime Monitoring
Quick-start Projects/ Code Accelerators
CoPA - Common Pipeline Architecture
‹WAG›
Workflow for Air-Gapped Deployment
Source Control & CI/CD
GitLab
Container & Artifact Management
Azure Container Registry
Sonatype Nexus
docker
container
Static Quality & Security Scanning
sonarqube
syft
Container & Compliance Scans
GitLab
OpenSCAP
NeuVector
Orchestration & GitOps
GitLab
argo
Packer
ChatOps
Mattermost
Logging/ SIEM
[Loki]
[Promtail]
Monitoring
Prometheus
Grafana
SPACE SYSTEMS COMMAND
Portability
Tool Agnostic
CNCF Kubernetes & Service Mesh
kubernetes
ISTIO
Azure AKS
P1 Big Bang
P1 Ironbank
Accreditation reciprocity
Focus on Mission vs. Operation
Security Engineered In
Cloud & On-Premises
Azure
Limit Vendor Lock
Accelerate Continuous ATO (cATO)
DoD DevSecOps Reference Design

Questions?

Thank You!

For more information, please contact:

Philip Chen
PM, Project Enigma
Phillip.chen@spaceforce.mil

Travis Dawson
GDIT PM, Project Enigma
travis.dawson@gdit.com

Dean LoNigro
PM, Project Enigma
dean.lonigro@spaceforce.mil

2026 SSC CYBER EXPO

S6/Program Protection

Partnering for Mission Assurance

Mr. Tony Terrazas, SSC/S6 Program Protection Branch Chief
Mr. Graham Jenkins, SSC/S6 Program Protection Deputy Branch Chief
Dr. Jess Smith, PNNL Cyber Security Engineer
Ms. Kayla Kwolek, PNNL Researcher

Agenda

- Introduction & Mission/Vision
- Our Core Services
- Why This Matters
- Questions & Open Discussion

Mission & Vision Overview

Our Team

SSC/S6 Program Protection Branch		
Name	**Grade**	**Role**
Manuel (Tony) Terrazas	NH-04	Branch Chief
Graham Jenkins	GG-13	Deputy Branch Chief
Erik Clary	GG-13	CI/SCRM Analyst
Marvin Leal	GG-13	CI/SCRM Analyst
Vacant	GG-13	CI/SCRM Analyst
Eric Bell	GS-11	Program Protection/SCRM Specialist
Brenda Taylor	CTR (ManTech)	Advisor
Ashlee Adame	CTR (PNNL)	Advisor
Cody Marcus	CTR (PNNL)	Advisor

Vision & Mission

Vision

Be the premier partner for all SSC programs and ensure that security and resilience are integral to every system lifecycle from day one, to guarantee mission success in contested, congested environments

Mission

Provide expert guidance, cutting-edge threat intelligence, and comprehensive support to safeguard SSC's critical technologies across its $15 billion acquisition portfolio

Core Services

Proactive Program Protection Support & Guidance

What We Do

- Partner with program offices to prepare, implement, and improve Program Protection Plans (PPPs)
  - Review statements of work and recommend program protection contracting requirements
  - Coordinate policy-driven PPP requirements, including threat assessments and counterintelligence support
- Drive criticality analysis standards and practices across the space enterprise
  - Help programs identify Critical Program Information (CPI) and Critical Components (CC)
  - Provide training on criticality analyses for CPI and CCs
- Guide programs through threat, vulnerability, and risk assessment processes
- Provide programs with a one-stop solution for meeting program protection requirements

We are not an audit function. We are your partners.

Actionable Threat Intelligence

Program Protection SCRM Analysis Cell:

- Core: three analysts with a collective 60+ years of intelligence, counterintelligence, and cyber experience
  - Augmented by FFRDC support (Pacific Northwest National Lab, Aerospace Corporation)
  - Close working partnership with Office of Special Investigations (OSI) Region 8
  - Broad contacts across the Intelligence Community and interagency
- Access to a wide range of government and commercial tools, databases, and other resources

What We Provide:

- On-demand threat briefings tailored to specific technologies, sectors, or vendors
- Supply chain risk and intelligence assessments
  - Shorter analyses of potential risks from companies under contract consideration
  - In-depth threat assessments for suppliers of critical components
- Trend analysis on threat actors and TTPs, counterfeit parts, and mitigation strategies

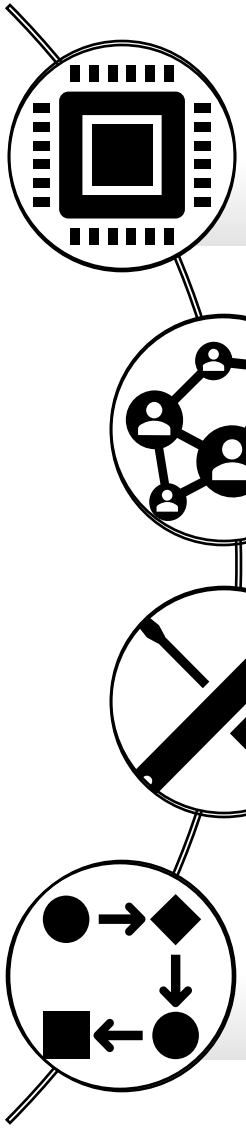
We deliver timely, relevant, and actionable intelligence for supply chain risk decisions.

Partner Capabilities

Pacific Northwest NATIONAL LABORATORY

Supply Chain Risk Management

Combining supply chain availability, integrity, and confidentiality for holistic and efficient risk management



Device Integrity

- Single-Unit Integrity
- Device enumeration and PAI research
- Hardware, software, and firmware deep dive investigations – full T&E

Systemic Integrity

- Multi-Unit Integrity
- Close support to actors in critical infrastructure
- Ensuring long-term availability of critical supplies or components

Policy and Structural Support

- Enabling foundational supply chain security
- Lifecycle maturity models, SCRM verification and validation for end users
- Systemic mitigations for device or organizational challenges

Entity Evaluations

- Corporate due diligence
- Product line-wide or manufacturer-wide integrity investigations
- Customized risk metrics

Why This Matters

Disrupting the Adversary

Supply Chain Threats: Three Main Categories

Acquisition

- Delayed/degraded production
- Lost IP
- Lost competitive advantage
- *Ex: Counterfeit hardware, hardware with embedded malware*

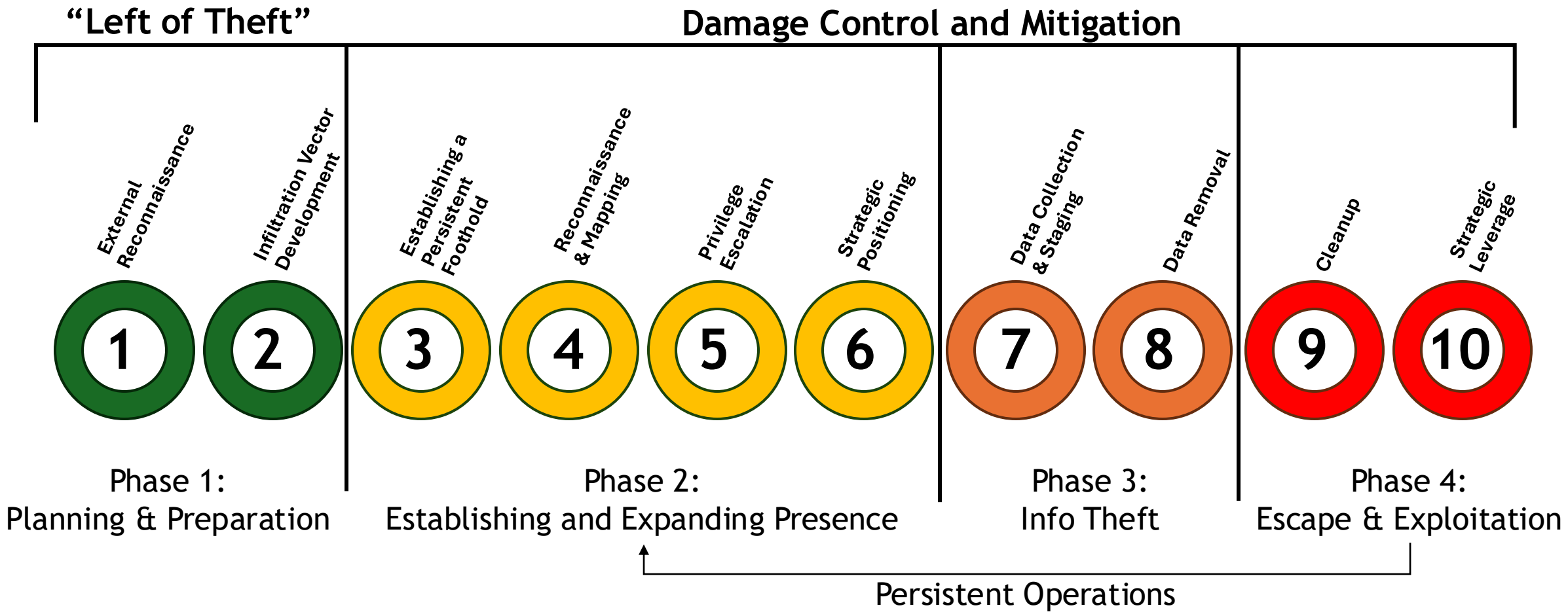
Cyber

- Compromised systems
- Exposed sensitive and national security information
- *Ex: Malicious code inserted into SolarWinds software (2020)*

Insider

- Disrupted operations
- Mission degradation
- *Ex: Tesla insider threat attempt (2020)*

The Adversary's Art of Exploitation



Defeating the Adversary

Phase 1: Planning and Preparation

- **Reduce Attack Surface -** Limit the amount of PAI about employees, technologies, and systems
- **Employee Training -** Train employees to recognize and report common methods used by adversaries
- **Security Assessments -** Conduct regular digital and physical vulnerability scans

Phase 2: Establish and Expand Presence

- **Intrusion Detection & Prevention -** Identify suspicious activity and alert security personnel
- **Enforce "Least Privilege" -** Grant access only to information and resources that are absolutely necessary
- **Monitor Network Traffic -** Watch for anomalies and signs of unauthorized access or data movement

Phase 3: Information Theft

- **Use Data Loss Prevention Tools -** Identify, monitor, and block the unauthorized transfer of sensitive data
- **Control Outbound Traffic -** Define "normal" outbound traffic to identify "low and slow" anomalous transfers
- **Incident Response Plan -** Contain the damage, eradicate the adversary, and recover operations

Questions?

Thank You!

For more information, please contact:

Your One-Stop Shop:

SSC.S6.ProgramProtection@spaceforce.mil

https://usaf.dps.mil/teams/ProgramProtectionSSCS6WorkingGroup

Initial Consultation:

“Not sure where to start? Request an initial consultation, and we’ll help you map out your program protection needs.“

https://usaf.dps.mil/sites/ussf-ssc/cio/SitePages/Cybersecurity.aspx?csf=1&web=1&e=MJPiAQ&CID=172ffe31-ead9-4950-9176-e0dec09244ca

2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

BREAK

VISIT EXHIBITORS!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Defensive Cyber Operations for Space DCO-S Capabilities

Mr. Steven Dominguez

6 STS/Technical Director, CFC MD 6

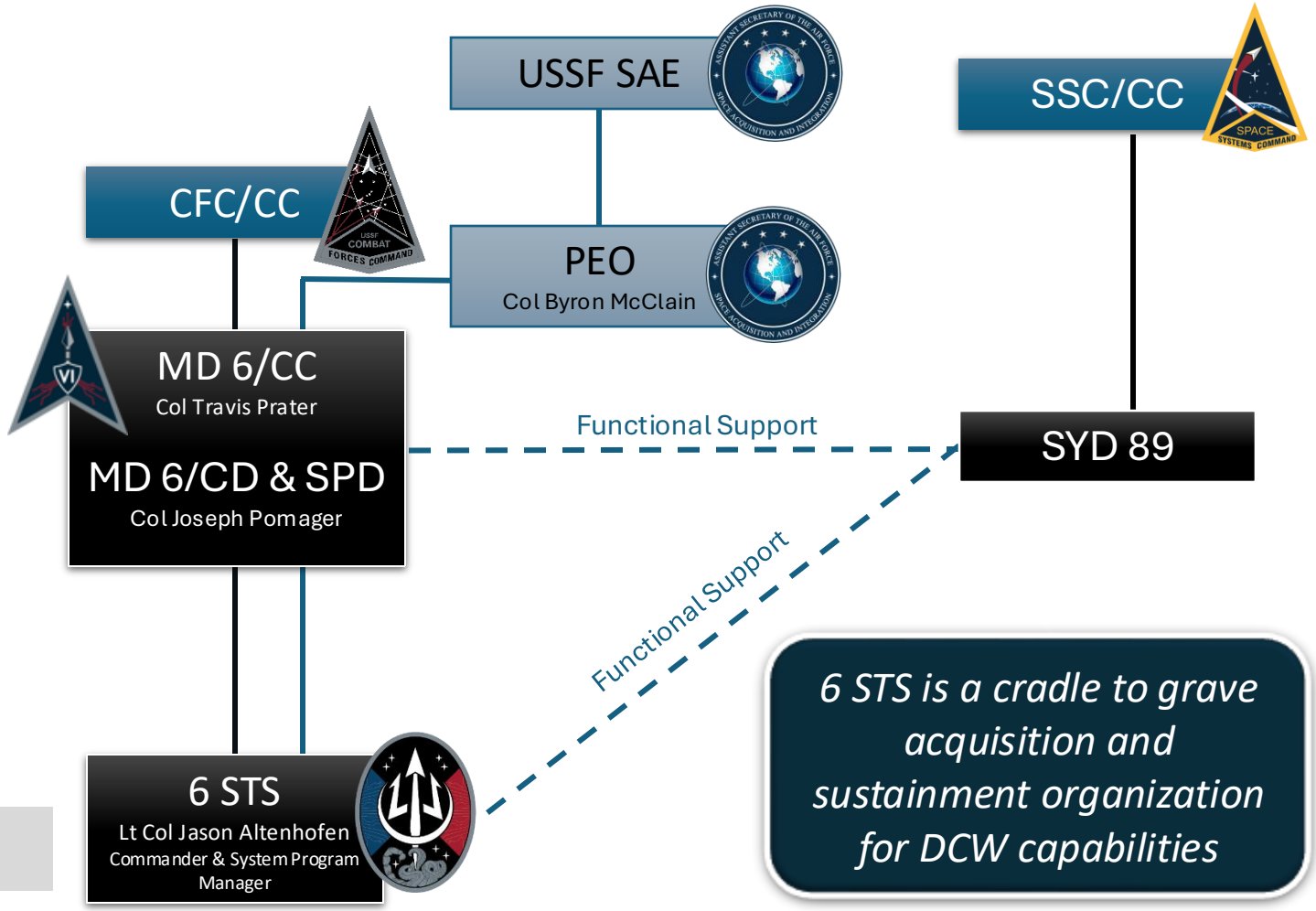
Cyber Readiness at the Speed of Space

Agenda

- Mission/Vision & Integrated Mission Delta Posture
- Key Partners
- Hub and Spoke Alignment
- DCO-S OV-1
- DCO-S Front Door

Integrated Mission Delta Posture (MD6)

- **Mission -** Rapidly field and enhance tools and capabilities to enable cyberspace warfare operations
- **Vision** - Combat-ready and responsive weapons that enable Space Force cyberspace operators to dominate the domain.



Truly an integrated provider to operational Cyber Guardians

Key Partners

USSF Mission Systems
(Deltas/PMOs/CYSs)

66 CWS
SOC

16 AF
USAF Cyber

AFRL/RV
SV Defense

SPACEWERX

AFLCMC/HN
CYBER & NETWORKS
mission execution directorate

USSF Field Commands

SPACE SYSTEMS
SSIO
INTEGRATION OFFICE

CCMDs
USSPACECOM
USCYBERCOM

ELICSAR
USAF Cyber BDP

NSA
TS Intel Feeds

Working across Space Force Mission Partners

Hub and Spoke Alignment

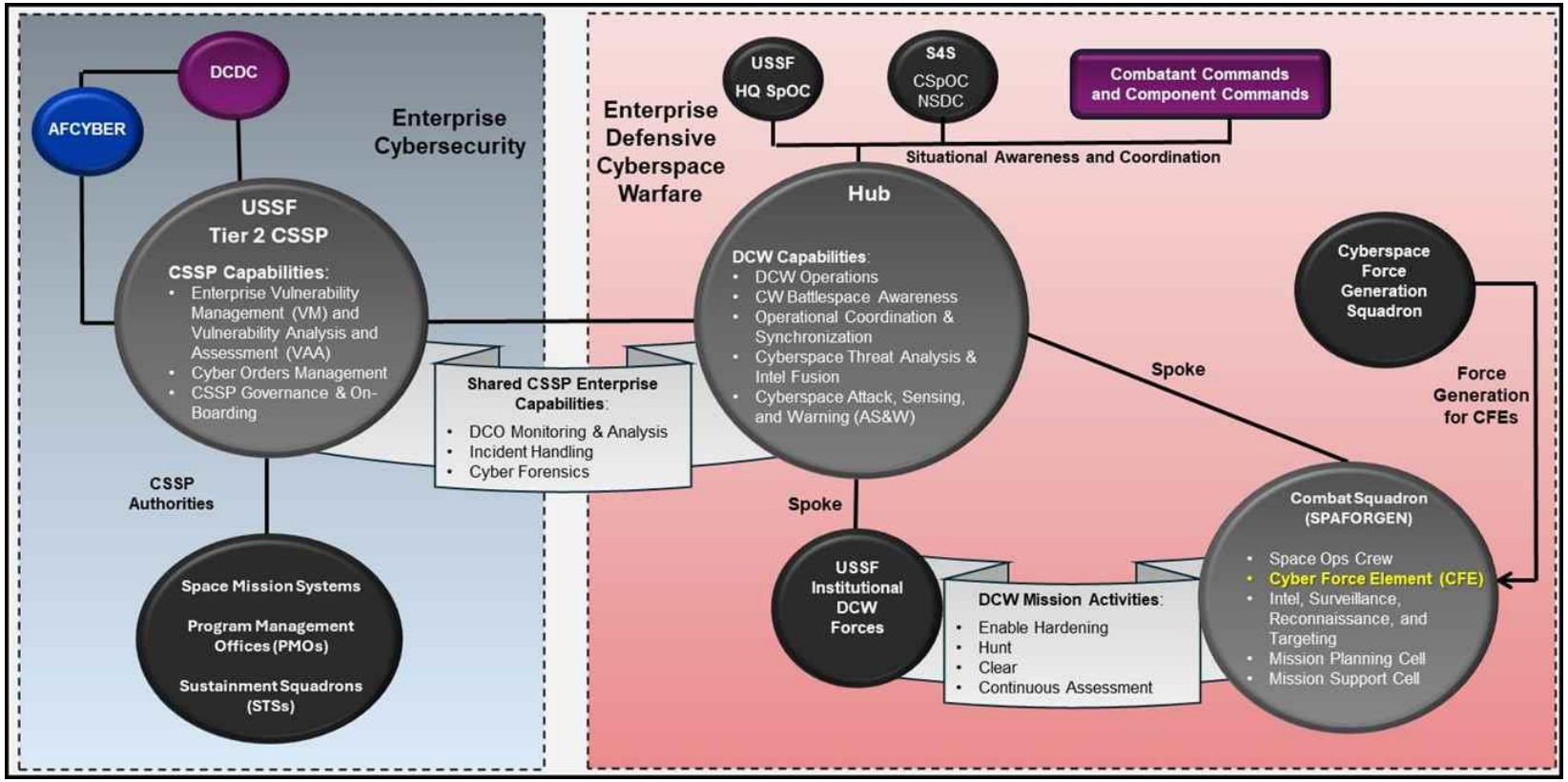
Our cybersecurity architecture is built on a 'Hub and Spoke' model to meet the dynamic needs of our cyber operators, integrating both centralized and mission-focused tools. We execute this in close alignment with our Cybersecurity Service Provider (CSSP) to ensure cohesive and robust defense across the mission landscape.

Enterprise-level enablement of:

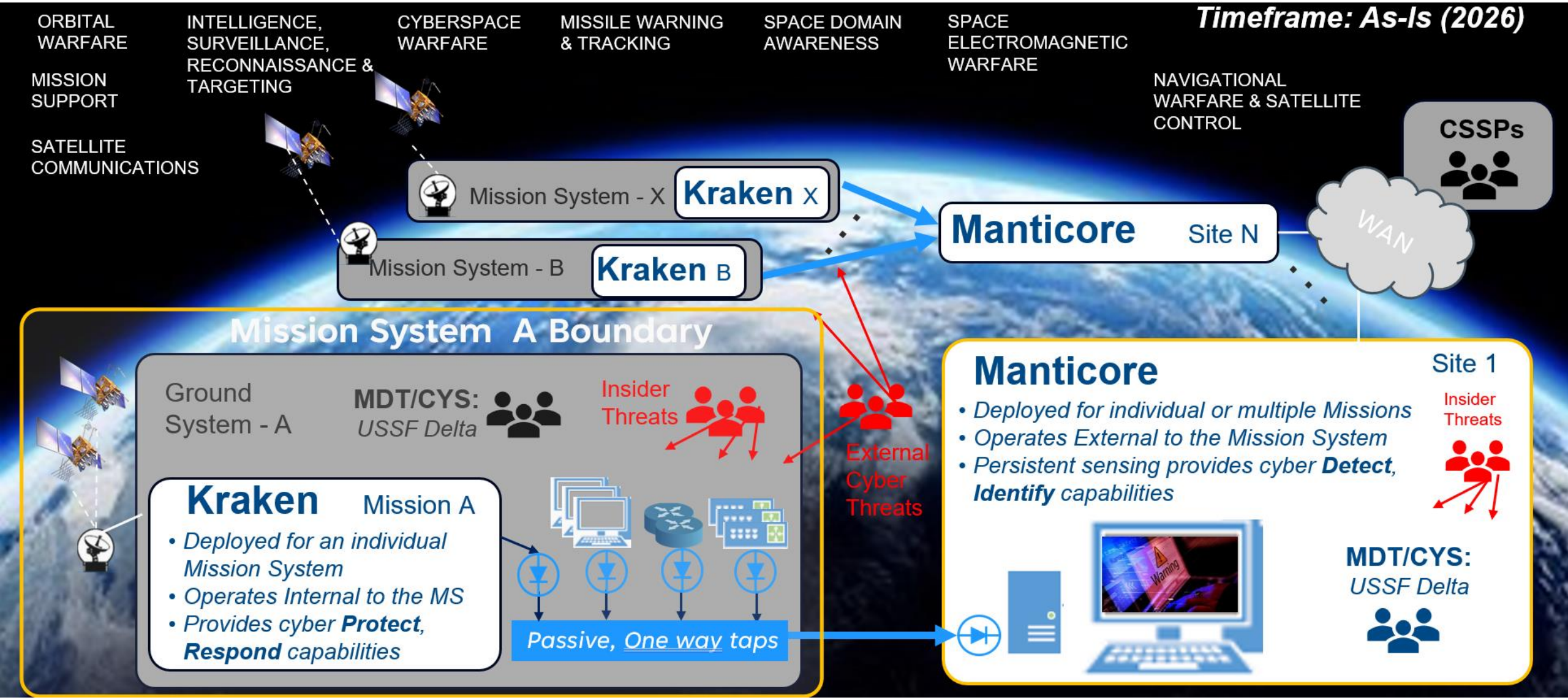
- Battlespace Awareness
- Ops Coordination & Synchronization
- Threat Analysis & Intel Fusion
- Attack Sensing & Warning (AS&W)
- Incident Handling & Forensics

Mission-boundary enablement of:

- Enable Hardening
- Threat Hunting
- Clear Operations
- Continuous Assessment



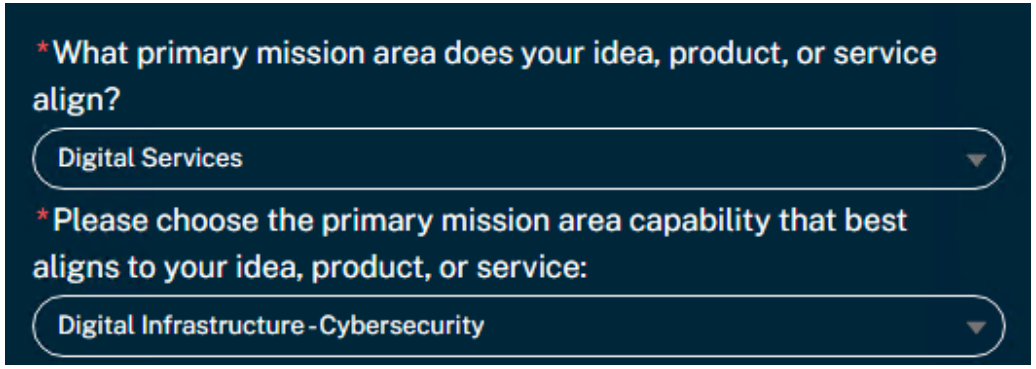
Defensive Cyber Operations – Space OV-1 (As-Is)

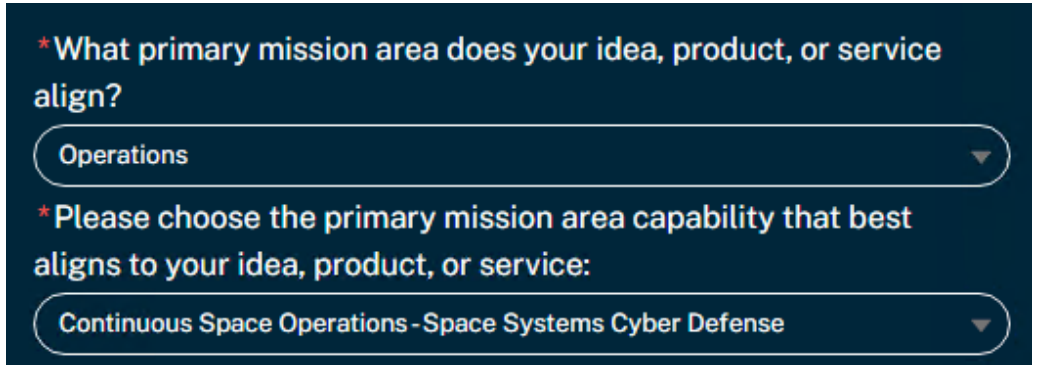


DCO-S Front Door

USSF Front Door Site

- **Establish a dedicated DCO-S sub-site on the USSF Front Door to provide a single, authoritative entry point for industry engagement.**
- **Leveraging the Front Door to track, manage, and deconflict all vendor interactions - ensuring transparency, continuity, and reduced churn.**
- **Implemented monthly Industry Day panel to rapidly evaluate innovative solutions against validated DCO-S mission needs.**





Submission details can be found here:
https://sscfrontdoor.experience.crmforce.mil/SSCFrontDoor/s/

Questions?

Thank You!

For more information, please contact:

Lt Col Jason Altenhofen
6 STS Commander
Jason.altenhofen.1@spaceforce.mil

MSgt Julio Santos Alvarez
6 STS Senior Enlisted Leader
Julio.santos_alvarez.1@spaceforce.mil

Mr. Steven Dominguez
6 STS Technical Director
Steven.dominguez.1.ctr@spaceforce.mil

6 STS Front Door
Squadron Strategic Engagement Interface
6sts.frontdoor.reqmgmnt@spaceforce.mil

2026 SSC CYBER EXPO

Delivering Cybersecurity Service Provider (CSSP) Capabilities

Mr. Craig Westerfield

CFC MD 6 Director, USSF CSSP

Cyber Readiness at the Speed of Space

Agenda

- **Cybersecurity Service Provider (CSSP) Overview**
  - Overview
  - CSSP Defined
  - CSSP Responsibilities
  - CSSP Authorities
- **CSSP Alignment**
  - CSSP Alignment Phasing
  - Navigating CSSP Alignment
  - External Services
- **USSF CSSP Cyber Tasking Orders (CTO)**
  - USSF C2 Cyber Relationships
  - CTO Process
- **Success Stories and Way Ahead**
  - Proven Success Stories
  - Cloud and SAP Strategies
  - Inspections and Assessments
- **Questions**

CSSP Overview

Overview

- **USSF CSSP currently located within the 66 CYS in Delta 6**
  - Delta 6 Commander: Col Travis Prater
  - 66 CYS Commander: Lt Col Bill Cosgrove
  - CSSP Director: Craig Westerfield
- **Manned by a mix of military, civilians, and contractors**
- **Mission Statement:** Provide cybersecurity support and defend space mission systems from ongoing or imminent threats in order to protect space component capabilities and enable power projection and freedom of action the space domain.

The Space Force's Digital Sword and Shield

CSSP Defined

CSSP

- **Provides cybersecurity services to owners of DoW information systems and/or computer networks to maintain and provide cyber situational awareness; implement protect measures; monitor and analyze to detect unauthorized activity; and implement cybersecurity operational direction (DoDI 8530.01)**

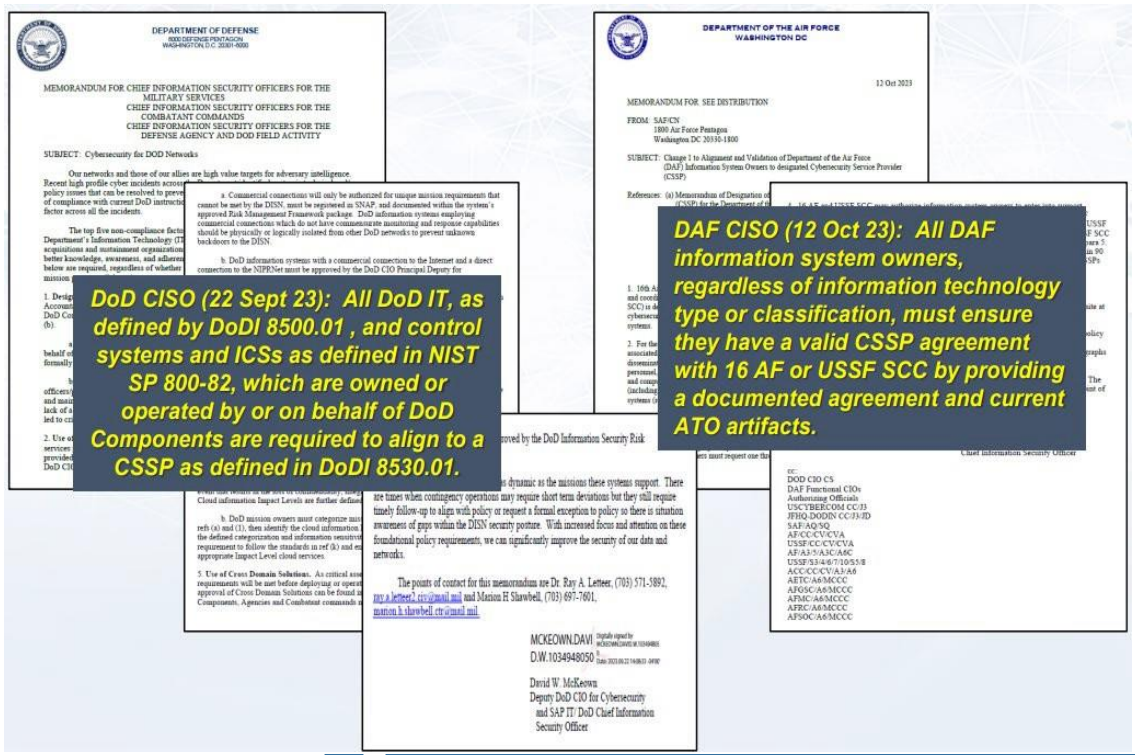
IAW DoDI 8530.01, DoD CSSPs will:

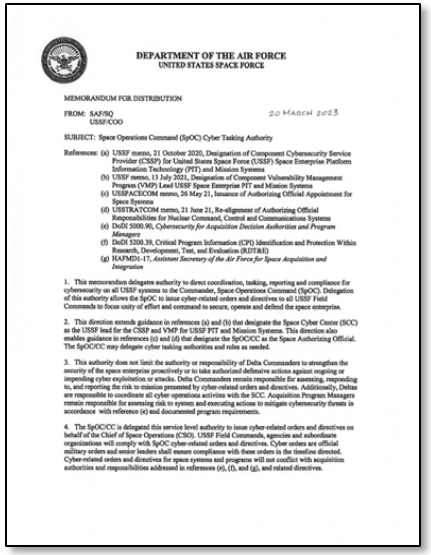
- **Provide cybersecurity services for the (NIST) cybersecurity framework functions**
- **Execute cybersecurity responsibilities and authorities IAW DoW policies, MOAs, contracts or support agreements**
- **Action USCYBERCOM and DCDC CTOs to ensure defensive cyber actions in managing network operations and cybersecurity activities**
- **Utilize MRT-C to understand and report on the criticality of cyber events and anomalies**

CSSP Responsibilities

- **Cybersecurity Policy and Guidance (Concepts, R&R, Plans, SLA/MOA/MOU, Training and Exercises)**
- **Component Cybersecurity Activities:**
  1. Vulnerability Assessment and Analysis
  2. Vulnerability Management
  3. Malware Protection
  4. Continuous Monitoring
  5. Cyber Incident Handling
  6. *DoDIN User Activity Monitoring (UAM) for the DoD Insider Threat Program
  7. Warning Intelligence and Attack Sensing and Warning (AS&W)
- **Reporting – Readiness, Cyberspace Operations, Cyber Incidents, Vulnerabilities**
- **Orders C2 – Triage, Development, Distribution, Tracking, and Reporting**
- **Forensics – Enterprise-level**
- **Lessons Learned – Facilitating, Development, Documenting, and Reporting**

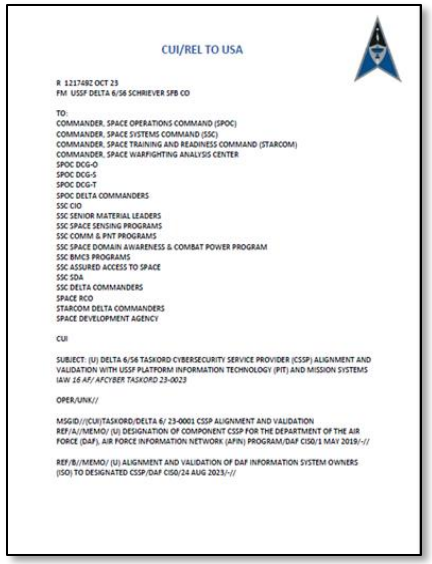
CSSP Authorities





SAF memo designates SpOC as USSF Tasking Authority and Delta 6 as USSF CSSP & VM Lead

AFCYBER Cyber Tasking Order 23-0023 requires all USSF Platform Information Technology (PIT) and Space Mission Systems to align to the USSF CSSP



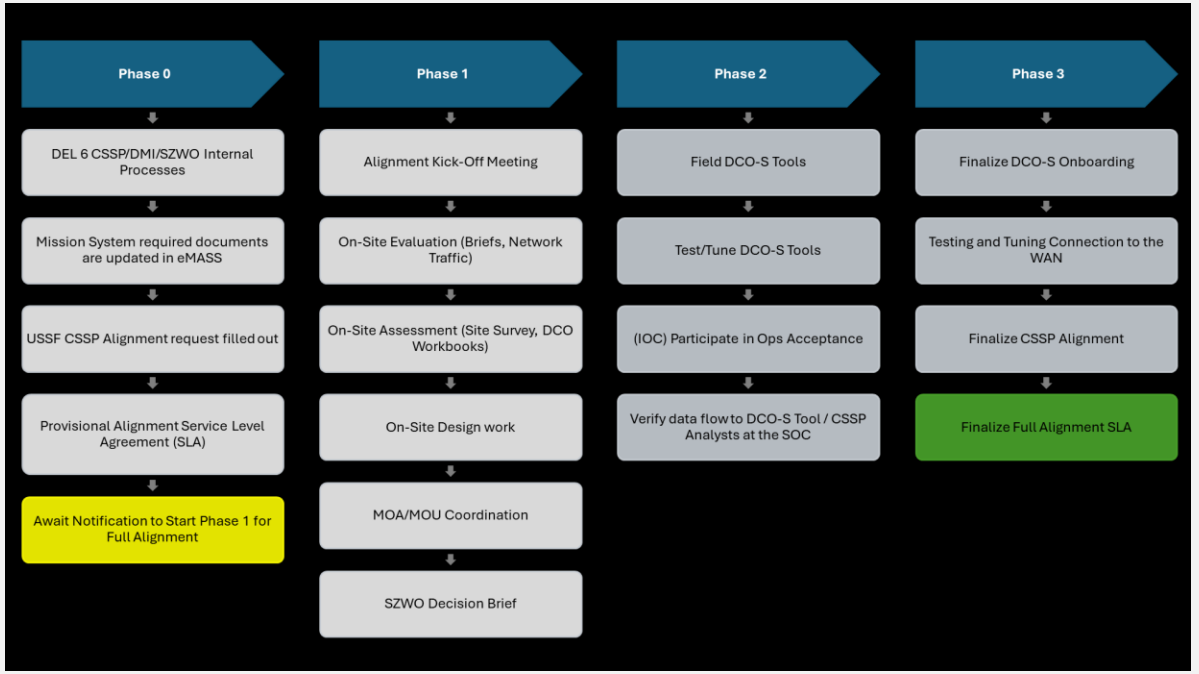
Delta 6/S6 Tasking Order 23-001 requires all PIT and Space Mission Systems to align to the USSF CSSP

DoD, USAF, and USSF directives issued to ensure the enterprise cyber defense through the alignment of PIT and Mission Systems to the USSF CSSP

CSSP Alignment

CSSP Alignment Phasing

- Phase 0: Provisional Alignment
  - Primarily conducted by CSSP Governance Team
  - Drives mission system requirements:
    - ACAS scan uploads in IKE
    - CTO Acknowledgement
- Phase 1: Initial Vetting and Integration
  - Primarily conducted by 6 STS
- Phase 2: DCO-S Tool Suite Deployment
  - Primarily conducted by 6 STS
- Phase 3: Full Alignment



To meet the intent of DoD and SAF alignment directives, system owners must collaborate with the USSF CSSP to execute the CSSP Alignment Policy and Checklist

Navigating CSSP Alignment

Provisional vs Full Alignment

- Provisional Alignment
  - Non-Technical CSSP Services: Cyber Threat Warning Intelligence, Vulnerability Management and Analysis, Incident Response
- Full Alignment
  - Technical CSSP Services: Continuous Monitoring, Insider Threat*, Malware Detection

CSSP Alignment Request - SIPR SharePoint

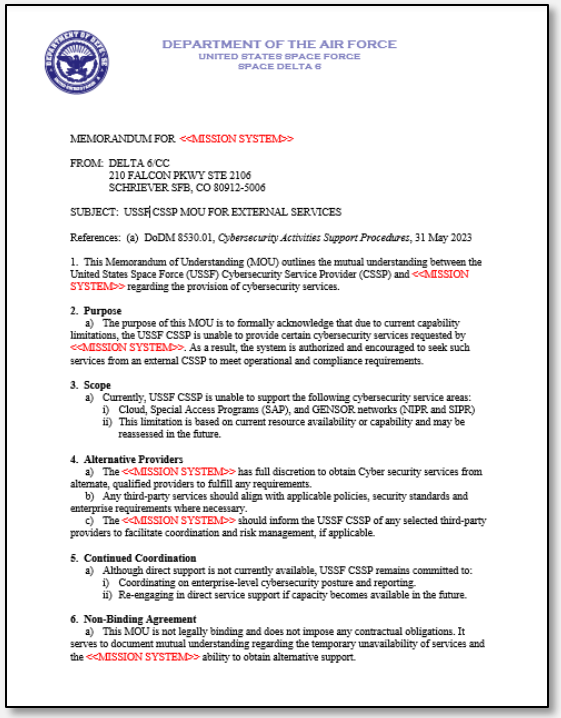
- All USSF Systems must submit a request
  - https://dod365sec.spo.microsoft.scloud/teams/usaf-ussf-spoc-del6
- Serves as initial notification to the USSF CSSP and a centralized location for exchanging information

Prioritization

- Internal schedule produced annually
- Exceptions to CSSP prioritization will occur on a case-by-case basis
- Systems not prioritized for DCO-S Deployment will be able to maintain a Provisional Alignment

External Services

- MOU between CSSP and System Owner
- CSSP documentation of limitation of services
- Unable to support GENSER environments
- Authorizes system owners to seek services from external CSSPs
- Third party CSSPs must have a current DCDC ATO and comply with all DoD governance
- System owners must provide third party CSSP info to the USSF CSSP
- Coordination between third party CSSP and USSF is required for USSF enterprise activity



DEPARTMENT OF THE AIR FORCE
UNITED STATES SPACE FORCE
SPACE DELTA 6

MEMORANDUM FOR <<MISSION SYSTEM>>

FROM: DELTA 6/CC
210 FALCON PKWY STE 2106
SCHRIEVER SFB, CO 80912-5006

SUBJECT: USSF CSSP MOU FOR EXTERNAL SERVICES

References: (a) DoDM 8530.01, *Cybersecurity Activities Support Procedures*, 31 May 2023

1. This Memorandum of Understanding (MOU) outlines the mutual understanding between the United States Space Force (USSF) Cybersecurity Service Provider (CSSP) and <<MISSION SYSTEM>> regarding the provision of cybersecurity services.

2. Purpose
a) The purpose of this MOU is to formally acknowledge that due to current capability limitations, the USSF CSSP is unable to provide certain cybersecurity services requested by <<MISSION SYSTEM>>. As a result, the system is authorized and encouraged to seek such services from an external CSSP to meet operational and compliance requirements.

3. Scope
a) Currently, USSF CSSP is unable to support the following cybersecurity service areas:
i) Cloud, Special Access Programs (SAP), and GENSOR networks (NIPR and SIPR)
ii) This limitation is based on current resource availability or capability and may be reassessed in the future.

4. Alternative Providers
a) The <<MISSION SYSTEM>> has full discretion to obtain Cyber security services from alternate, qualified providers to fulfill any requirements.
b) Any third-party services should align with applicable policies, security standards and enterprise requirements where necessary.
c) The <<MISSION SYSTEM>> should inform the USSF CSSP of any selected third-party providers to facilitate coordination and risk management, if applicable.

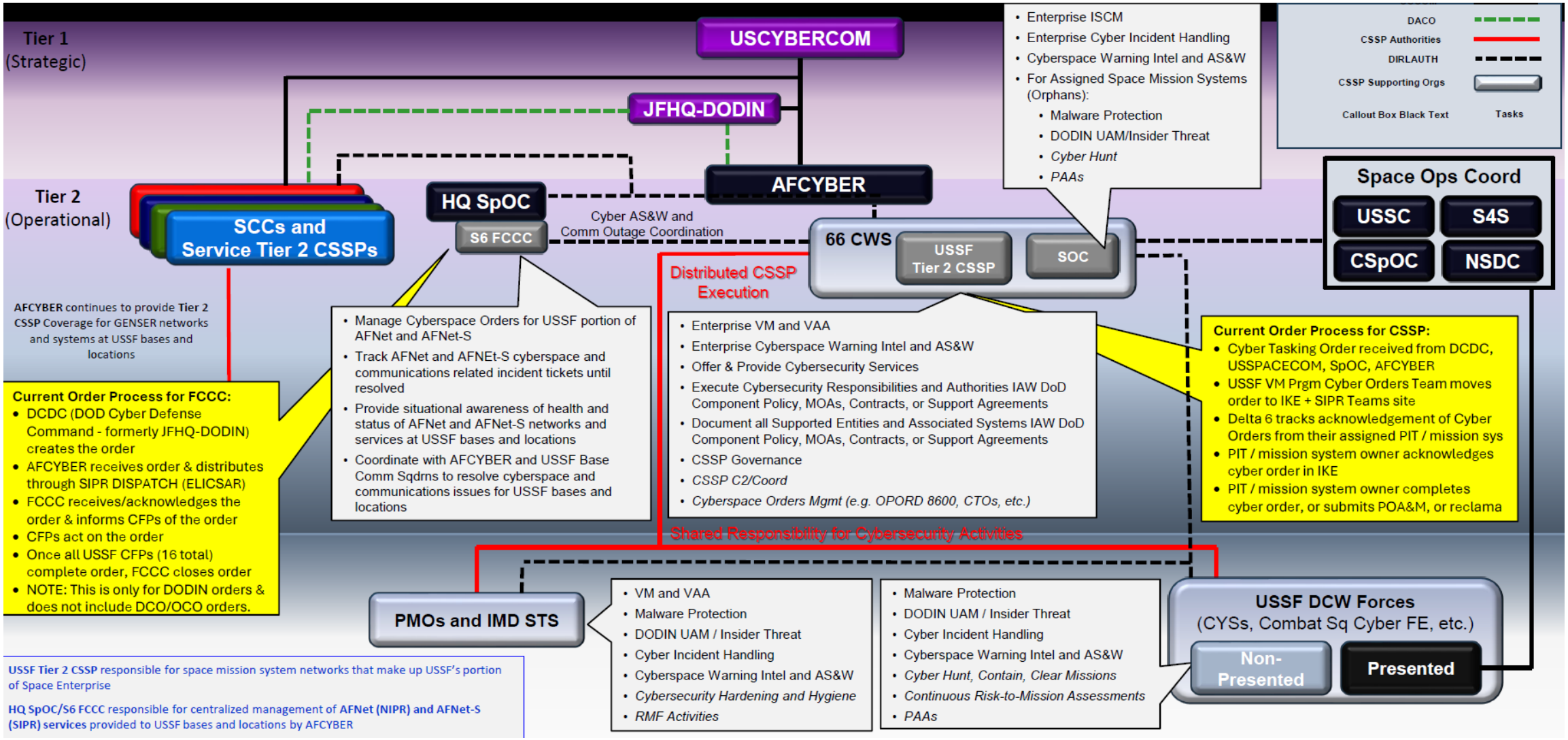
5. Continued Coordination
a) Although direct support is not currently available, USSF CSSP remains committed to:
i) Coordinating on enterprise-level cybersecurity posture and reporting.
ii) Re-engaging in direct service support if capacity becomes available in the future.

6. Non-Binding Agreement
a) This MOU is not legally binding and does not impose any contractual obligations. It serves to document mutual understanding regarding the temporary unavailability of services and the <<MISSION SYSTEM>> ability to obtain alternative support.

The intent is to ensure mission systems can immediately obtain required CSSP coverage. USSF may gain additional services in the future requiring changes to third party agreements.

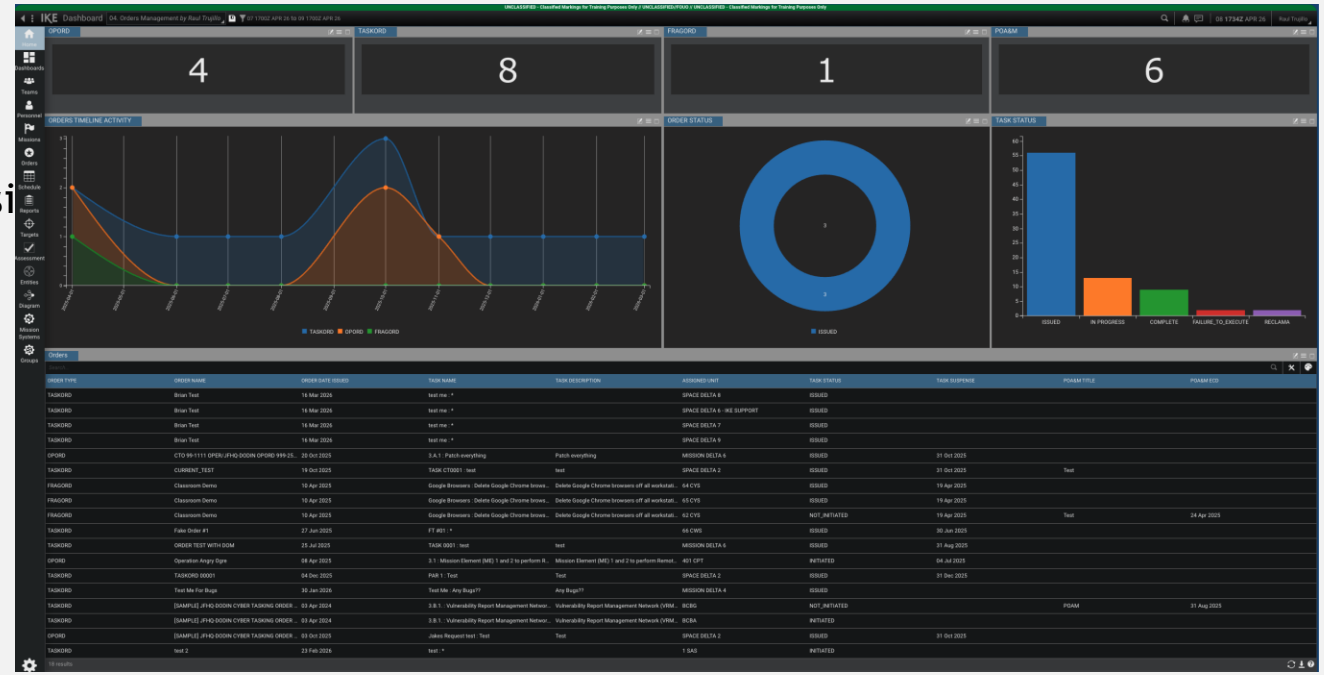
USSF CSSP
Cyber Tasking Orders (CTO)

USSF C2 Cyber Relationships



CTO Process

- Cyber Tasking Order received from DCDC, USSPACECOM, CFC, or AFCYBER
- USSF Cyber Orders Team moves order to IKE with notification on NIPR Teams si
- Mission system owner acknowledges cyber order in IKE
- USSF Cyber Orders Team tracks CTO acknowledgement and reports at Cybersecurity Working Group (CSWG)
- Mission system owner completes cyber order, marks as not applicable, or submits POA&M in IKE



The identification and analysis of disclosed vulnerabilities to determine their associated risk and potential operational impact to the space enterprise.

Success Stories and Way Ahead

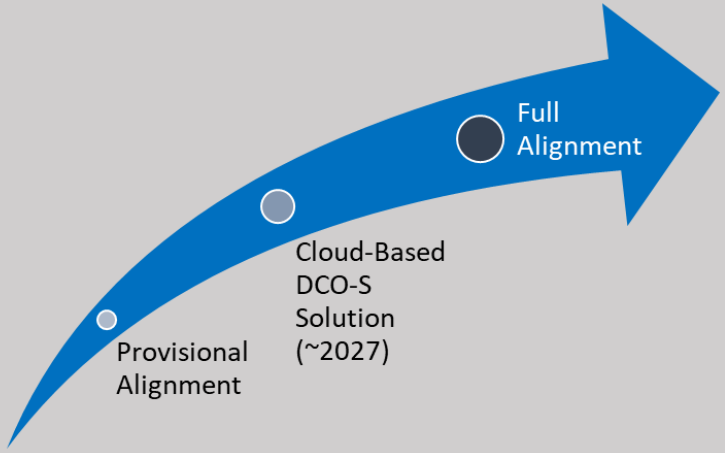
Proven Success Stories

- 2025 DCDC CSSP Assessment – 100% “Center of Excellence”
  - 156 Evaluators Scoring Indicators across Identify, Protect, Detect, Respond, Recover
- 2025 Resolved Operational Weaknesses in Cyber Orders Management
  - AF Auditing Agency: “this is the model example for how to resolve systemic deficiencies”
  - Doubled Space Mission System Cyber Orders throughput & 50% increase in Compliance
  - Initiated Hardening Orders from Cyber Protection Team Mission Findings - 70% Acknowledgment Rate
- 2025 Mission System CSSP Alignment Portal Launched: 1,100% engagement increase
  - Current Status: 159/327 Enclaves Captured
- Mission System Index (MSI) Established
  - Authoritative inventory of all USSF Mission Systems and Enclaves below SAP & Developmental levels
- Cyber Warfare Common Operating Picture (COP) Launched

Cloud and SAP Strategies

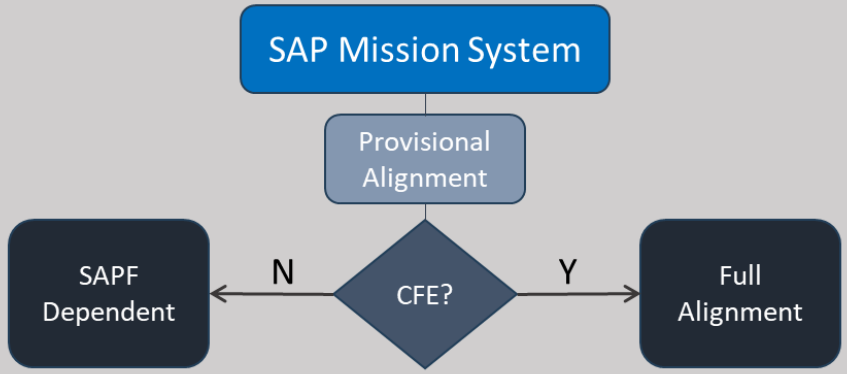
Cloud Strategy

- Establish Provisional CSSP Alignment to cloud-based Mission Systems with the intent to deploy a cloud-based DCO-S solution (i.e., Manticore/Kraken) as it becomes available (~2027 timeline)
- Provides Non-Technical CSSP Services in the interim



Special Access Program (SAP) Strategy

- SAP reads for CSSP Governance personnel
- Establish Provisional CSSP Alignment to SAP Mission Systems
- Full Alignment for SAP Mission Systems with assigned Cyber Force Elements (CFE)
- Full Alignment for SAP Mission Systems without assigned CFEs are SAPF dependent



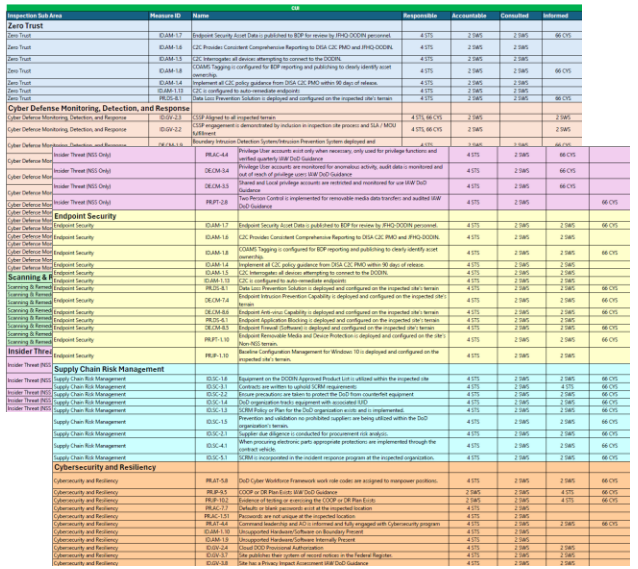
Inspections and Assessments

AF Auditing Agency

- 2025 resolution of previous repeat findings of operational weaknesses in cyber orders management was only possible due to the outstanding cooperation between SYD85 and the CSSP Cyber Orders Team
- This audit had GO-level visibility but at the end of the day was resolved by AOs with determination to succeed

Cyber Operational Readiness Assessment

- DOD Cyber Defense Command (DCDC) mandated that the Cyber Assessment Team at 16 AF (16AF/CAT) conduct a Cyber Operational Readiness Assessment (CORA) on 2 SWS/MD 4.
- This assessment is functionally equivalent to a Command Cyber Readiness Inspection (CCRI) and the first of its kind for a dedicated space mission system.
- Although 2 SWS is the designated unit, CORA will effectively assess sustainment and security posture provided by the 4th Sustainment Squadron (4 STS).
- This establishes a new precedent and signals DCDC's intent to standardize defensive cyber assessments over all DoD mission/weapon systems.



USSF Points of Contact

NIPR

- Alignment Portal
  - https://usaf.dps.mil/sites/SpOC-DEL6/home/ussfcssp
- Email
  - Delta6.CSSP.ALL@spaceforce.mil
- SharePoint
  - https://go.mil/uo0zhq2f7o
- Microsoft Teams
  - https://go.mil/ov11f49pja

SIPR

- Alignment Portal
  - https://dod365sec.spo.microsoft.scloud/teams/usaf-ussf-spoc-del6
- Email
  - ussf.schriever.del-6.mbx.s-63-cssp@mail.smil.mil
- SharePoint
  - dod365sec.spo.microsoft.scloud/teams/USAF-USSF-SpOC-DEL6/SitePages/Alignment
- IKE
  - space.ike.us.af.smil.mil

The Mission System Index, or the “Phone Book for Mission Systems”, is available on the SIPR Alignment Portal.

Questions?

Thank You!

For more information, please contact:

Lt Col William Cosgrove
66 CYS Commander

Craig Westerfield
USSF CSSP Director
Craig.westerfield@spaceforce.mil

MSgt Nathan Lynch
CSSP Flight Chief
nathan.lynch@spaceforce.mil

2026 SSC CYBER EXPO

On Orbit Cyber Defense
Secure by-Design Space Vehicles

Mr. Joseph "Dan" Trujillo DR-3

Air Force Research Lab Space Cyber Resiliency Program Lead

Cyber Readiness at the Speed of Space

Overview

Why is Space Cyber Different?

Protection of Legacy Space Vehicles

Future Space Architecture & Missions

Vision for the Next-Generation of Cybersecure and Resilient Space Vehicles

Why is Space Cyber Different?

- **Mission-specific designs that prevent standardization**
- **Physics that couples software to irreversible orbital dynamics**
- **Permanent loss of ability to fix/modify hardware after launch**
- **Communication gaps that mandate autonomous decisions**
- **Environmental degradation of electronics**
- **Tight subsystem dependencies that enable cascading failures**

Cybersecurity that treats mission continuity and availability as first-order design and security primitives rather than adopting from terrestrial

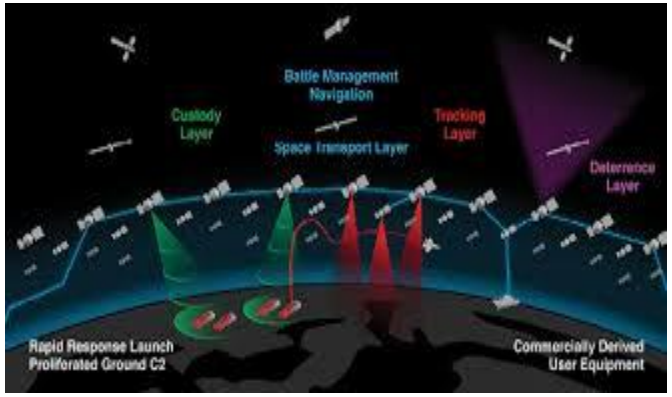
Space vehicles require mission-centric cybersecurity

Legacy Space Vehicle Cyber Protection

- **On-orbit assets can only accept software updates "bolt-on"**
  - **Therefore, making it difficult to properly design-in needed security**
- **Properly and safely implementing onboard autonomous response**
  - **Designs do not include cyber requirements with respect to compute**
  - **Could be harmful while competing for compute resources**
  -
- **"Bolt-on" defenses do not FIX the problem -> Ex. Detection**
- **Effects due to faults and/or space weather can show up as cyber-attacks -> response needs to be appropriate**

Ex. GPS Constellation

Future USSF Space Architecture & Missions

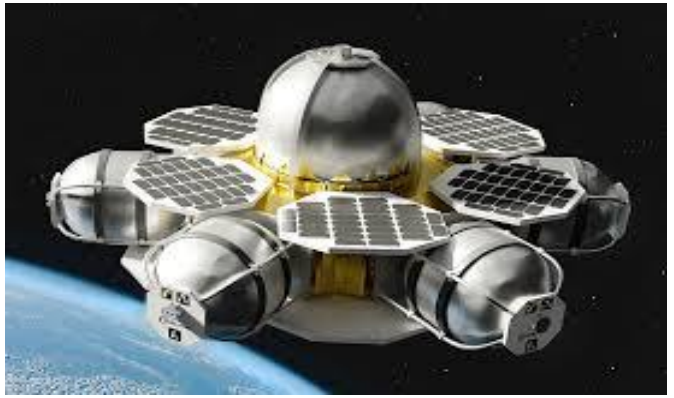


Proliferated Warfighter Space Architecture (PWSA)

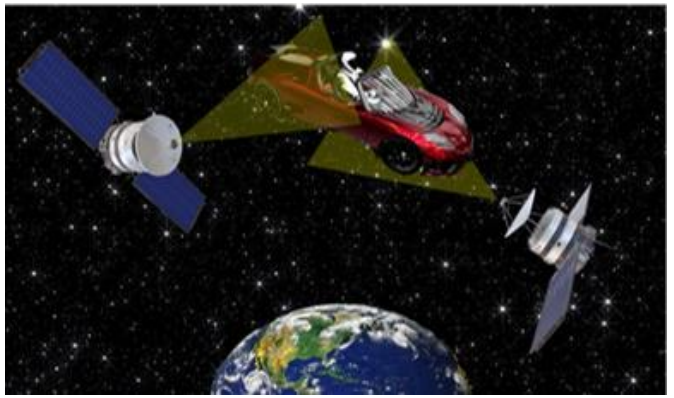
Golden Dome

Starshield & Starlink

Autonomy/Lights-out



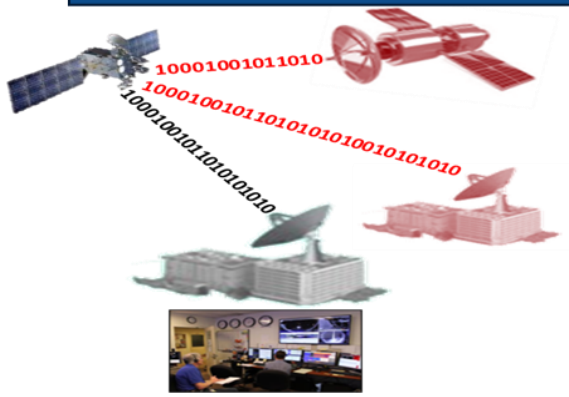
On-Orbit Servicing/Refueling



Muli-Agent/Cooperative/ Inspection

Increasing Attack Surface

Legacy & Current → **Future Capabilities** → **Increasing Attack Surface & Vulnerabilities**



- H/W & S/W supply chain
- Bugs
- Malware
- Open source/COTS trustworthiness

+

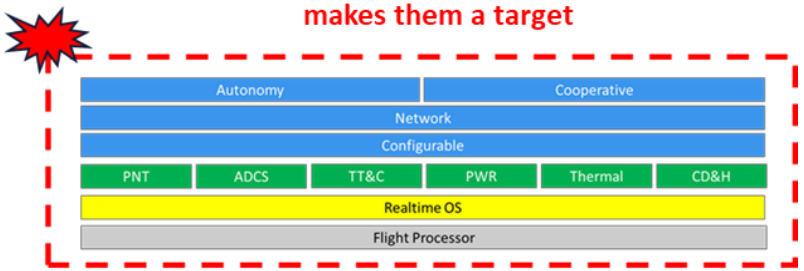
- Multi-Agent/Cooperative missions
- Autonomous systems
- Fully reconfigurable missions

- Constellations/Networked/Hybrid
- Integrated Air & Ground networks

- Decisions and Response on the Edge
- Sensor Data generation/Processing

=

Increasing critical capability on space vehicles makes them a target



Next-Gen Space Vehicle Flight Software Stack

We want to keep our critical satellite systems, C2, and data secure, AND we want to greatly expand operational flexibility through integrated architectures

BUT this will vastly increase cyber-attack surfaces and vulnerabilities …

Comprehensive Space Vehicle Cybersecurity and Resiliency

Security

- Hardened trusted core
- Reduce attack surface
- Reduce impact in case of compromise
- Flexible architecture allowing for mission posture
- Allow integration of Resiliency Mechanisms

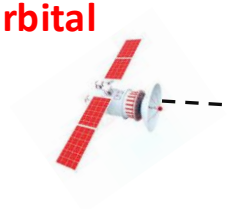
Resiliency

- Detection
- Protection
- Recoverable
- Adaptable

Next-Gen Cybersecure & Resilient Space Vehicles

A foothold on the space vehicle that allows the DCO be alerted to cyber-attack, isolates, and provides mechanisms for protection and recovery

Co-orbital



Supply Chain, Insider, compromised

- Space Vehicle Self-Protection
- Space Vehicle Cyber Situational Awareness

Manticore/Kraken cyber Tools

Cyber Ground C2 Defensive Cyber Operations - Space

ENTERPRISE – Cyber Situational Awareness

Onboard capability for Space Cyber

Ground-based

Design Choices

- **Modular Architectures:**
  - **Implementation of cyber protections (ZT, Least-Priv.)**
  - **Isolation of processes**
  - **Granular detection**
  - **Granular recovery (update & restart)**
  - **Granular testing**
- **Adaptable Architectures**
- **Flexible architectures for mixture of onboard and offboard execution and response**
- **Safe autonomous response**

Cyber system-of-systems must work seamlessly within the space vehicle and mission systems

2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

BREAK

VISIT EXHIBITORS!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Judgment Under Operational Pressure

Strengthening Decision Quality in Cyber & Space Environments

Dr. Hugo Velazco
SSC SYD89/SYA

Cyber Readiness at the Speed of Space

Agenda

- Pressure Is Not the Risk
- Predictable Human Effects Under Pressure
- Operational Scenario
  - Three Conditions That Protect Judgment
  - What Changes in the Two-Hour Window
- Judgment Is a Strategic Asset

Pressure Is Not the Risk

- Pressure is constant in cyber and space operations.
- What creates mission risk is degraded judgment under load.
- Drivers of pressure today:
  - Increasing cyber threat velocity
  - AI-accelerated decision cycles
  - Cross-functional technical complexity
  - Compressed leadership timelines

Under stress, human judgment is a system vulnerability.

Predictable Human Effects Under Pressure

Under sustained pressure, decision environments shift in predictable ways:

- Attention narrows
- Urgency replaces prioritization
- Communication shortens
- Defensive loops emerge

None of these indicate failure.

They are normal human responses to pressure accumulation.

Ignoring predictable human factors is a direct threat to mission success.

Operational Scenario

A vulnerability is identified in a mission-critical system 48 hours before a milestone review.

Inputs conflict across technical teams.
Risk thresholds are unclear.

Leadership requests a status update in two hours.

The problem is not information.

The problem is decision stability under pressure.

Train for decision making under pressure with the same rigor we apply to technical training.

Three Conditions that Protect Judgment

1 Signal Discipline

- Distinguish verified information from assumption.

2 Decision Framing

- Clarify what must be decided now versus later.

3 Cognitive Expansion

- Ensure the team’s full expertise informs the decision.

What Changes in the Two-Hour Window

Signal Discipline

- What information is confirmed versus inferred?

Decision Framing

- What decision is actually required before the milestone review?

Cognitive Expansion

- Whose perspective is missing from the discussion?

Judgment Is a Strategic Asset

AI accelerates analysis and output.

Humans retain accountability for decisions.

Mission reliability ultimately depends on decision quality under pressure.

Pressure will remain constant.

Judgment must be protected.

The cognitive ability of our leaders is a warfighting capability.

Questions?

Thank You!

For more information, please contact:

Dr. Hugo Velazco
Space Systems Command Support
hugo.velazco.ctr@spaceforce.mil

2026 SSC CYBER EXPO

Innovation Lab

Accelerating Innovation for the Warfighter, Digital Transformation

- **Mr. Tony Uminn,** Digital Transformation Director, Patrick SFB
- **Mr. Derek Eichin**, Chief Data Officer, Space Launch Delta 30
- **Mr. Eric Kemp**, Sr. Enterprise Software Architect, Space Launch Delta 30
- **1st Lt Patel,** Flight Commander, Combat Forces Command

Cyber Readiness at the Speed of Space

Agenda

- **SLD 45 Innovation Space, The Forge**
  - Mission & Vision
  - Projects & Gaps
- **SLD 30 Innovation Space, The Crucible**
  - Mission & Vision
  - Projects & Gaps

SLD 30 Innovation Space, The Crucible

Mission

- Recognize and empower innovative leaders in every unit to collaborate, share, and accelerate needed change.
- Foster an experimental mindset that allows for fast implementation, fast learning, and accepts failure.

Vision

- A Space Launch Delta where we quickly unleash new technology, schools of thought, and set the USSF standard for innovation adoption.
- Foster an environment where innovation is enabled, expected, and routine.

Projects & Gaps

Lead Projects and Events

- Launch and Test Range Capacity Modeling
- 3D Printing for Operational Systems
- MSFT Hosted Applications & SW Dev
- AI & Data Visualization Workshops & Expos
- Red Cell Cyber Exercises
- Data Fusion for Command and Control

Gaps

- Software Virtualization Technology
- Space Launch and Test Event ADS
- Legacy Coding Language Converters
- Wargaming Offerings
- Engineering Large Language Models
- Predictive Cybersecurity Issue Monitors

SLD 45 Innovation Space, The Forge

THE FORGE
Space Launch Delta 45 ⚡ Space Spark 1

Mission

- Unite our military, industry, and academic talent to build the data-driven foundation for mission-critical change.
- Create a seemless innovation ecosystem for solving Space Lift Range challenges.

Vision

- A digital ecosystem empowering Guardians and partners to solve challenges, and accelerate capabilities.
- Cultivate a data-driven, tech-forward culture that leverages frontier technology to outpace the evolving threat.

Projects & Gaps

Lead Projects and Events

- 45 DTO hosted Supra Coder Dev Team
- 3D printed Ops sensor guard (Stevenson Screen)
- DCTC / Hacking 4 Defense Acedemia Partnership
- Launch Count Update Board 2.0 (L-CUB)
- Common Operational Data Infrastructure (CODI) Next Gen
- Watercraft Authentication & Visual Evaluation System (WAVES)

Gaps

- A digial intake portal for DTO engagement
- Digital twin of the Eastern Range (Mod & SIM)
- Legacy Coding Language Converters
- Excellerated scaling capabilities
- OTA Ability for Quick Tool Acquisition

Questions?

2026 SSC CYBER EXPO

Network Social

SOUTH BAY
BAR & GRILL

3:45

Grab a drink coupon from a sponsor

Thanks to our Sponsors!

August Schell	NetScout	MoonTiger	Space Force Association
Google	Red River	Viasat	
Illumio	Rise8	VioletX	

Feedback Survey

Cyber Readiness at the Speed of Space