2026 SSC CYBER EXPO

April 21-23

Gordon Conference Center

LA Air Force Base

WELCOME TO

Day 1 | Tuesday, April 21

Strategic Vision meets Operational Excellence.

event website

Cyber Readiness at the Speed of Space

Day 1: Strategic Vision Meets Operational Excellence

Morning Schedule

0900 - 0905	Introductions
0905 - 0920	Welcome Remarks Col Andrew Menschner
0920 - 0950	Keynote Address Ms. Charleen Laughlin
0950 - 1030	Panel: Space Force Field Command leaders unpack emerging cyber capabilities, operations, & strategic roadmaps / alignment
1030 - 1045	Break! Visit Exhibitors
1045 - 1130	Panel: SSC Delta Leaders tackle mission-readiness from Ground, to Launch, to Orbit
1130 - 1200	Leveraging Cyber Ranges and Aggressor Capabilities for Operational Advantage
1200 - 1300	Lunch Break | Complimentary Lunch Voucher

Special Guest Speaker

Day 1: Strategic Vision Meets Operational Excellence

Afternoon Schedule

1300 - 1345	Panel: Advancing the Cyber Workforce with Mission Ready Talent
1345 - 1415	Government Reference Architecture for Space Vehicle Hardening and Defense Solutions
1415 - 1430	Break! Visit Exhibitors
1430 - 1450	Maturing Space Sensing through Digital Engineering
1450 - 1530	Mission Application of Continuum and Quantum Computing
1530 - 1600	Panel: Government & Defense Contractor Cybersecurity Risk Management Updates
1600 - 1605	Closing Remarks

Enjoying the Expo?
Give us Feedback
Scan the QR Code

Detailed agenda on website

2026 Special Guest Speakers

Day 1

Col Andrew Menschner

Deputy Commander
Space Systems Command

Ms. Charleen Laughlin SES 3

Deputy Chief of Space Operations for Cyber & Data
HQ USSF S6

Day 2

Dr. Keith Hardiman SES 2

Deputy Director
DAF CIO

Mr. John Weiler

CEO & CIO
IT-Acquisition Advisory Council (IT-ACC)

Day 3

Dr. Jose Angeles

Chief Data Officer
U.S. SOUTHCOM

Ms. Alissa Knight

Founder, CEO, and Chief AI Officer of Assail, Author, 6x Award Winning TV Producer

2026 SSC CYBER EXPO

Welcome Remarks

Col Andrew Menschner
SSC Deputy Commander

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Keynote Address

Ms. Charleen Laughlin
Deputy Chief of Space Operations for Cyber & Data
HQ USSF S6

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

Leadership Panel

USSF Leaders unpack emerging cyber capabilities, strategic roadmaps, the evolving cyber concept of operations, and Enterprise alignment

Moderator: TSgt Michaela Sosville, SSC/S6

Panelists:

- Col Brian Mihalko, SSC/S6 Director
- Mr. Charlie Brown, SSC/S6 Deputy Director
- Col Sung In, SSC/S6 Chief of Staff
- Col Robert Enrico, SSIO Enterprise Capabilities
- Lt Col Andrew Buchanan, 68 CYS Commander

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

Panel | SSC System Delta Leadership

From Ground, to Launch, to Orbit, the System Deltas (SYD) and Space Launch Deltas (SLD) discuss what it means to be mission-ready in 2026 and beyond.

Moderator: Ms. Minh Jones (MJ), SSC Acquisition Specialist

Panelist:

SLD 45	Col Chatman, Commander
SBD 3	Mr. Jeffrey Curry, Director of 61 Comm Squad
SYD 80	Mr. Josh Jackson, Chief Engineer
SYD 84	Mr. Eric Mattessich, Chief Engineer
SYD 831 & 88	Mr. Dean LoNigro, S6/Chief, Cyber Threat Response/ISSM
SYD 81	Mr. Albert Yates, Chief Cyber Engineer &
	Mr. Steve Mink, System Integration Engineer

System Delta Info Graphic

Cyber Readiness at the Speed of Space

SPACE SYSTEMS COMMAND DELTAS

SSC is the U.S. Space Force field command that develops and delivers dominant, integrated, and resilient space warfighting capabilities, protecting our Nation's strategic advantage in, from, and to space.

Current as of FEB 2026

DEL: SPACE DELTA
MD: MISSION DELTA
PAE: PORTFOLIO ACQUISITION EXECUTIVE
PEO: PROGRAM EXECUTIVE OFFICER
SBD: SPACE BASE DELTA
SLD: SPACE LAUNCH DELTA
SYD: SYSTEM DELTA

SLD 30 - VSFB

SLD 45 - PSFB, CCSFS

SBD 3 - LA AFB

PAE & PEO RELATIONSHIPS

SYD-TO-DELTA PARTNERSHIPS

SPACE ACCESS	OPERATIONAL TESTING & TRAINING INFRASTRUCTURE	SPACE SENSING	MILITARY COMMUNICATIONS & POSITIONING, NAVIGATION & TIMING	SPACE COMBAT POWER	BATTLE MANAGEMENT, COMMAND, CONTROL, COMMUNICATIONS, & SPACE INTELLIGENCE
SYD 80	**SYD 81**	**SYD 810**	**SYD 84**	**SYD 88** / **SYD 831**	**SYD 89**	**SYD 85**
SPACE ACCESS	OPERATIONAL TEST & TRAINING INFRASTRUCTURE (OTTI)	SPACE-BASED SENSING & TARGETING (SBST)	SPACE-BASED MISSILE WARNING & TRACKING (SBMWT)	SATELLITE COMMUNICATIONS (SATCOM) / NAVIGATION WARFARE & PNT (NAVWAR)	SPACE COMBAT POWER (SCP)	BATTLE MANAGEMENT, COMMAND, CONTROL, COMMUNICATION, & SPACE INTELLIGENCE (BMC3I)
SLD 30, SLD 45	DEL 1, DEL 10, DEL 11, DEL 12		MD 2, MD 4, MD 8, MD 31, MD 6, DEL 7, MD 3, MD 9		DEL 5, DEL 15

SPACE SYSTEMS COMMAND DELTAS

SSC is the U.S. Space Force field command that develops and delivers dominant, integrated, and resilient space warfighting capabilities, protecting our Nation's strategic advantage in, from, and to space.

SLD 30 - VSFB

SLD 45 - PSFB, CCSFS

SBD 3 - LA AFB

Current as of FEB 2026

DEL: SPACE DELTA
MD: MISSION DELTA
PAE: PORTFOLIO ACQUISITION EXECUTIVE
PEO: PROGRAM EXECUTIVE OFFICER
SBD: SPACE BASE DELTA
SLD: SPACE LAUNCH DELTA
SYD: SYSTEM DELTA

PAE & PEO RELATIONSHIPS

SYD-TO-DELTA PARTNERSHIPS

SPACE ACCESS	OPERATIONAL TESTING & TRAINING INFRASTRUCTURE	SPACE SENSING	MILITARY COMMUNICATIONS & POSITIONING, NAVIGATION & TIMING	SPACE COMBAT POWER	BATTLE MANAGEMENT, COMMAND, CONTROL, COMMUNICATIONS, & SPACE INTELLIGENCE

SYD 80

SPACE ACCESS

- SLD 30
- SLD 45

SYD 81

OPERATIONAL TEST & TRAINING INFRASTRUCTURE (OTTI)

- DEL 1
- DEL 10
- DEL 11
- DEL 12

SYD 810

SPACE-BASED SENSING & TARGETING (SBST)

SYD 84

SPACE-BASED MISSILE WARNING & TRACKING (SBMWT)

- MD 2
- MD 4

SYD 88

SATELLITE COMMUNICATIONS (SATCOM)

- MD 8
- MD 31

SYD 831

NAVIGATION WARFARE & PNT (NAVWAR)

- MD 6
- DEL 7

SYD 89

SPACE COMBAT POWER (SCP)

- MD 3
- MD 9

SYD 85

BATTLE MANAGEMENT, COMMAND, CONTROL, COMMUNICATION, & SPACE INTELLIGENCE (BMC3I)

- DEL 5
- DEL 15

2026 SSC CYBER EXPO

Leveraging USSF Cyber Ranges and Aggressor Capabilities for Operational Advantage

Capt Skyler Hart

STARCOM 33rd RGS

Dir. Range Operations

Cyber Readiness at the Speed of Space

Agenda

- Overview of 33d Range and Aggressor Squadron
- Cyber Range overview
- Capabilities under development

33d RGS Overview

Location: Schriever SFB, CO

Leadership Team:

- Commander - Lt Col Brandon Wilson
- Deputy Commander - Maj Eric Merriss
- SEL - MSgt Stephanie Scheerer

33d RGS Overview

Mission

To prepare Guardians for war by providing expert Cyber Range, Aggressor, and Intelligence capabilities, and by knowing, teaching, and replicating advanced adversary cyber threats to support SPAFORGEN readiness and training.

Strategic Objectives

The squadron is focused on three primary lines of effort: preparing Guardians for conflict, establishing our own operational baseline, and partnering to deliver cutting-edge capabilities.

- Prepare Guardians for War: Provide comprehensive Cyber Range, Aggressor, and Intelligence capabilities for SPAFORGEN readiness cycles, Flashpoints, and other Service-level training events.
- Develop Advanced Capabilities: Actively partner with the Operational Test and Training Infrastructure (OTTI) to co-develop and deliver the next generation of Cyber Range and Aggressor capabilities.

Core Aggressor Functions

We execute our mission through the classic "Know, Teach, Replicate" aggressor model, applied specifically to the cyber domain.

Know:

- Maintain expertise on the latest cyber vulnerabilities, exploits, and proofs-of-concept for network and system exploitation.

Teach:

- Participate in and deliver adversary threat briefs and share lessons learned from training events to improve friendly force TTPs.

Replicate:

- Realistically replicate adversary tactics, techniques, and procedures (TTPs) against a variety of target sets, meeting customer needs on custom ranges.

33 RGS Overview

NRO*

CFC

S4S

STARCOM

SSC

CCMDs

Delta 26

MQT/AT/Exercises:
Delta 26 OSD
660 COS
661 COS
662 CYS
662 CYS Det 21
663 CYS
664 CYS
664 CYS Det 44

Delta 6

MD6:
66 CYS (CWOC)
66 CYS FTF
66 CYS Det 1

Delta 7

Cyber Threats:
74 ISRS

IMDs & C2 Deltas

Con/Mon & Hunt:
62 CYS
64 CYS
68 CYS
69 CYS
631 CYS
NSDC
CSpOC

Delta 1

Officer/Enlisted Training Course (OTC/ETC):
533 TRS Det1
319 CTS

Delta 11

R&A Ops:
33 RGS

Scenario Dev, EX:
392 CTS

Delta 12

SF Cyber Testers:
Cyber Flights in 1 TES, 3 TES, 4 TES, 14 TES, 17 TES

AF Cyber Testers:
(available via ITF)
346 CTS, 47 CTS
48 CTS

SYD 81 (OTTI)

Range Dev:
TIP-C

Infra:
TIF

SPOs and PMOs

Test Customers:
SPOs & PMOs

SZ

DCO-S Developer:
SZYO

ICS/SCADA Cyber Tools Developer:
SZYN

DCO Units

Assess, Harden, Hunt, Clear CMR:
645 CYS
630 CYS

Future Space Service Component Command & JFHQ-C

CMF Teams:
Red Team, Assessment Prep, Mission Rehearsal

CPTs presented to S4S:
901 CPT
902 CPT

NRO/SpOC/S4S Training Users

TRS/CTS, R&A, Test

Program Offices & Training Users

Joint Users

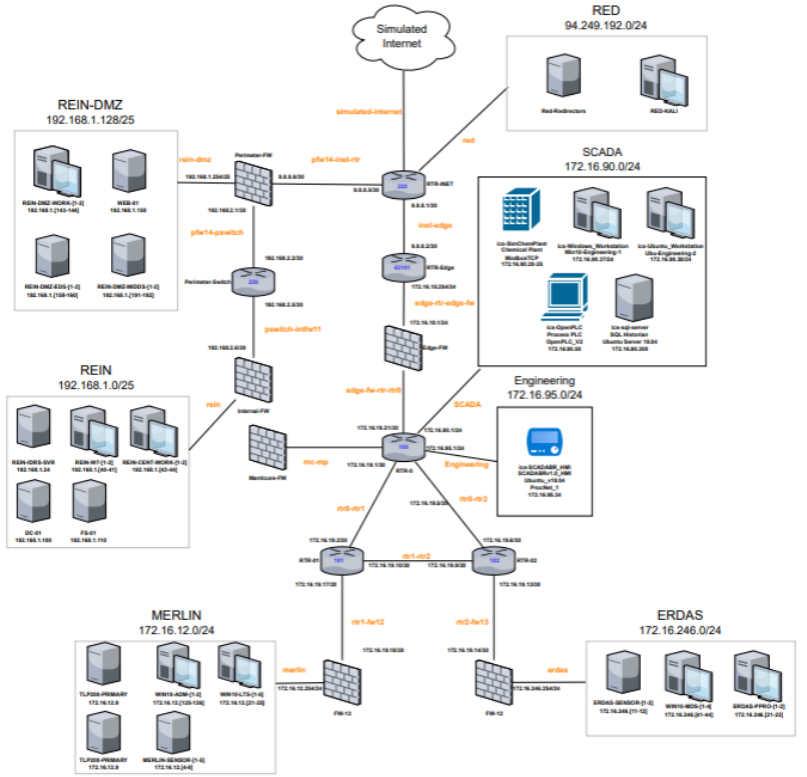
** NRO does not have USSF units, but Cyber Guardians have training needs at those units*

SF Staff:
Demonstration

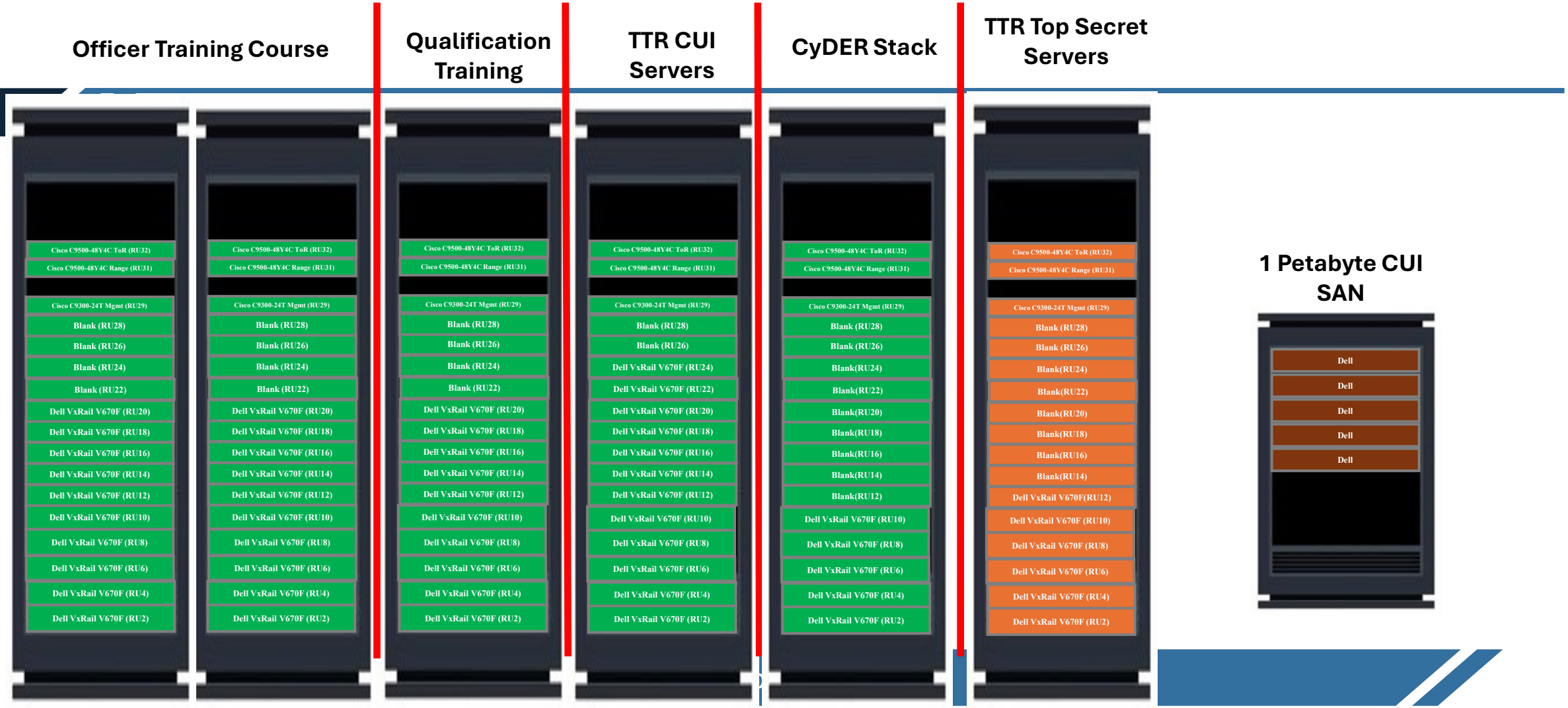
Cyber Range Overview

What Range services do we provide?

- Realistic Space cyber terrain using virtual machines (user emulation, simulated internet, OS considerations, ICS/SCADA)
- Closed system
- Unclass/CUI and Top Secret
- Accessible through web browsers via Foundry and Player
- Cyber Tools
  - Manicore 1.21
  - Splunk
  - Security Onion
  - Open source tools
  - etc.



33d RGS Range: Infrastructure



Cyber Range Overview

Officer Training Course

- Persistent Range provided to 319th CTS
- New Officers learn basics of cyber
- GradEx capstone exercise
- Supports 60 students per cohort

Qualification Training

- Persistent Range provided to 66 CYS/FTF
- Host Cyber Defense Operator (CDO) course
- Developing Incident Responder course and Differential Training course
- Supports 180 students per year

Cyber Range Overview

Texas Training Range (TTR) CUI

- By-request range (PI-SOC)
  - CT, AT, CRV, LFEs, SEP events
- High-fidelity but usually not mission relevant terrain
- Highly customizable
- Live OPFOR support (33d Aggressors)
- 61 Test/Training/Exercise events in FY25

- LFE: Space Flag/Red Flag
- CRV: Vermillion Stars
- CT/AT: Cosmic Axolotl/individual requests
- 120 day lead time for Range & Aggressor support
- 45 day lead time for Range only support

Cyber Range Overview

CyDER

- Persistent on-demand range
  - CT & AT
- Low-fidelity mission relevant terrain
- Longer lead time for changes
- Automated attack-chains
  - CYS's are able to instruct and be red team
- Quickly reset range

- 8 CyDER deployed: SMP, SBIRS, SC2NET, CCIC2S, AEHF, W-LTRS, E-LTRS
- 6 Automated attack chains
- Host 20 students per event

Cyber Range Overview

CyDER Automated Attack example

- **Phase 1:** Initial Recon & Access
- **Phase 2:** Internal Recon & Pivot
- **Phase 3:** Privilege Escalation & Persistence
- **Phase 4:** Mission System Manipulation
- **Phase 5:** Data Theft

Capabilities in Dev

CyDER & TTR on TS

- Developing High-fidelity mission relevant terrain.
- Needs to be accessed through a Joint Information Operations Range (JIOR) node

Other

- Integration of HWIL
- LFE TS Ranges
- Various hardware upgrades
- Transfer of DARK SKIES and CVPA modules to TTR
- NOS3 & COSMOS

Questions?

Thank You!

Lt Col Brandon Wilson
Commander

MSgt Stephanie Scheerer
SEL

Maj Eric Merriss
Deputy Commander

Capt Skyler Hart
Director, Range Ops

Dining Options
Tuesday, April 21st

BX Restaurants:
Tenkatori
Gusto's

Food Trucks
Chicken King
Family Pizza
Dip Deez Ice Cream

South Bay Bar & Grill
Buffet Special
Enchilada Casserole
Rice & Beans
Salad & Beverage

CHICKEN KING

SOUTH BAY
BAR & GRILL

THE FAMILY PIZZA
NY STYLE
SINCE 2020

SPACE SYSTEMS COMMAND

S6

LUNCH

Complimentary $15 lunch voucher with registration.
Use at Food Trucks, South Bay Grill, or BX Food Court

See you at 1300!

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

PANEL

Advancing the Cyber Workforce with Mission-Ready Talent

Moderator: TSgt Lee Harder, SSC/S6

Panelists:

- Mr. Matt Isnor, DoW Cyber Workforce Development Director
- Mr. Timothy Beard, DAF Associate Career Field Manager, Cyber and IT
- Ms. Desirre Lorell, USSF HQ/S6 Workforce Director
- CMSgt Rajab Kigembe, SSC/S6 SEL
- Ms. Aine Nakai, S6 Workforce Development Lead

2026 SSC CYBER EXPO

Government Reference Architecture for Space Vehicle Cyber Hardening and Defense Solutions

Capt Adeeb Islam, SSIO Cyber Integration, Chief

Mr. Andy Walther, SSIO Cyber Architectures & Integration

Cyber Readiness at the Speed of Space

UNITED STATES
SPACE FORCE

Integrating the Space Enterprise

Capt Adeeb Islam
Cyber Integration, Chief

Integrate to Dominate!

SSC Org Chart

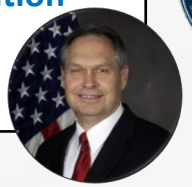
DAF PEO C3BM
Maj. Gen. Luke Cropsey

HQE
C3BM Chief, Architecture & Systems Engineering
Dr. Bryan Tipton

Assistant Secretary of the Air Force for Space Acquisition and Integration ASAF (SA&I)
(Vacant)

Military Deputy ASAF (SA&I)
Maj. Gen. Stephen Purdy
(Acting ASAF (SA&I))

HQE
Senior Advisor to the SAE (SASAE) SA for Space C2 & Integration (SASC2I)
Mr. James Haywood



Space Deputy

DISES
SSIO Civilian Deputy
Ms. Kris Acosta

SSIO Director
Col. Jon Strizzi

SSIO Military Deputy
Col. Jeremy Selstrom

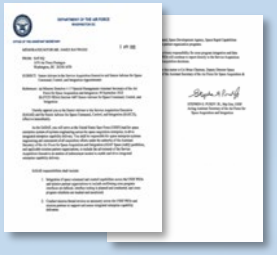
Enterprise Capabilities & Modernization
Col. Robert Enrico

NH-04
Mission Enterprise Integration
Mr. Al Matos

NH-04
Enterprise Engineering & Governance
Mr. Mark Honda

NH-04
SSIO Operations Management
Ms. Mia Cafi

Space Systems Integration Office Requirements and Reviews



NDAA

Administration Priorities

SASAE & SASC2I Appointments

Ensure integration of space C2 capabilities across USSF PEOs, PAEs, SSC SYDs, & mission partners

FY25 National Defense Authorization Act (NDAA) Section 1607 (Space C2 & Integration)

Provide architecture & integration support to C3BM PEO

Conduct mission thread reviews

Recommend Program Objective Memorandum (POM) investment priorities

Coordinate and execute systems engineering control boards for system-to-system interfaces

Improve PEO/PAE/SYD integrated capability delivery

Primary Products

- Design Reference Mission (DRM)
- Integrated Requirements Doc (IRD)
- Enterprise Integrated Schedules
- Integrated Assessment (Strategy/Plan)
- Mission Engineering Thread (MET)

Enterprise Mission Integration and Analysis

- POM Priority Recommendations
- Space Enterprise Governance
- Enterprise Integration Memos (EIM)
- Enterprise Standards
- Digital Ecosystem (DEco)
- Foundational Cross-cutting Capabilities

Enterprise Technical Governance and Requirements

- USSF Science & Technology (S&T) Prioritization

Space Futures Tech

SSIO products will influence future requirements through based on Industry Capability

Space System Cyber Life Cycle: The New Paradigm to Ensure Mission Operations

Program Start → **Reduce Vulnerabilities** → **Maintain Strong Cybersecurity Measures** → **Actively Defend** → End of Life

Data Exfiltration & Exploitation Threats Persistent Across Life Cycle

Design & Build

Vulnerabilities mitigated during development

Deploy

System not compromised during deployment

Operate

Active defense of mission & mission support sys

Sustain

Secure Pipeline to evolve and adapt to threats

Disposal

Sanitized, nothing left for exploitation

Courtesy graphic by MITRE

SSIO Focus Areas

Enterprise Capabilities & Modernization
Col. Rob Enrico

- **Cyber Integration**
- Crypto Modernization
- Spectrum Management & Space Environment
- Industrial Base & Supply Chain
- Digital Ecosystem & Artificial Intelligence

Mission Enterprise Integration
Mr. Al Matos

- Ops Analysis
- Integrated Requirements Document
- Enterprise Integrated Master Schedules
- Integrated Assessments Strategy / Report
- Risks, Issues, & Gaps
- DAF Battle Network ICDs & AO / ATOs *(C3BM Support)*
- Mission Engineering Threads & MBSE
- Design Reference Missions

DAF: Department of Air Force
ICDs: Interface Control Document
AO/ATO: Authorization to Operate
MBSE: Model Based Systems Engineering

Enterprise Engineering & Governance
Mr. Mark Honda

- Enterprise Governance
- Integration Command Media
- Integration Enforcement
- Enterprise Technical Baseline

SSIO Deliverables and Products

Enterprise Capabilities & Modernization
Col. Rob Enrico

- **Cyber Integration**
- Crypto Modernization
- Spectrum Management & Space Environment
- Industrial Base & Supply Chain
- Digital Ecosystem & Artificial Intelligence

Cyber Enterprise Mission Engineering Primary Products

- Design Reference Mission (DRM)
- Integrated Requirements Doc (IRD)
- Enterprise Integrated Schedules
- Integrated Assessment (Strategy/Plan)
- Mission Engineering Thread (MET)

Enterprise Mission Integration and Analysis

- Objectives
  - Establish, document & lead assessment of cyberspace warfare Design Reference Missions
  - Develop Mission Engineering Threads for defensive cyberspace warfare mission set
  - Capture Risks, Issues and Gaps in the METs and operational implementations
  - Build Integrated Requirements for the defensive cyberspace warfare mission set

Cyber Enterprise Requirements & Future Tech Primary Products

- POM Priority Recommendations
- Enterprise Standards
- Foundational Cross-cutting Capabilities
- USSF S&T Prioritization

Enterprise Technical Governance & Requirements

Space Futures Tech

- Objectives
  - Identify Space Vehicle Cyber Technology Gaps and Priorities
  - Provide data to support SSIO S&T portfolio and Air Force Research Laboratory (AFRL) Investment decisions
  - Develop Space Vehicle (SV) Cybersecurity Requirements and Standards for future systems

These efforts culminate to posturing the Space Enterprise to protect and defend against emerging threat landscape

Evolution of Space Cybersecurity

Space was a Sanctuary

- High Cost of Escalation
- Physically Hard to Attack
- Radio Frequency (RF) Jamming
- Classified, Proprietary Systems
- Very Little Commercial Off The Shelf (COTS)

- “Hard Shell, Soft Interior”
- Isolated Networks
- Reliant on Encryption

Evolution

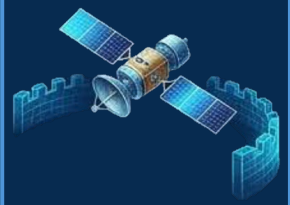
New Cyber Threats & Vulnerabilities

- Advanced Persistent Threat (APT)
- Insider Threats
- Automation/Artificial Intelligence Enabled Attacks
- Quantum Computing Threats
- Inter-connected Architectures and Data Sharing
- COTS Solutions
- RF-Enabled Cyber Threats
- Operational Technology/Industrial Control Systems Vulnerabilities
- Supply Chain/Dev Env Vulnerabilities
- Critical Infrastructure Vulnerabilities
- Change Management Vulnerabilities

Enterprise-Wide Vulnerabilities

Space System Attack Vector Triad

SPACE SEGMENT



ATTACK SURFACE

- Command Spoofing / Injection
- Malicious Firmware
- Legacy Hardware /Software(HW/SW) Exploits
- Supply Chain Compromise

LINK SEGMENT

ATTACK SURFACE

- Data Exfiltration & Eavesdropping
- Replay Attacks
- Signal Jamming (Up/Down & Cross-Links)
- RF-Enabled Cyber Attacks

GROUND & USER SEGMENT

ATTACK SURFACE

- On-prem & Cloud Data & Information Technology (IT) Networks
- Critical Infrastructure
- Supply Chain Attacks & Dev Environment
- OT/ICS Systems

Modern Threat Landscape

- Commercial Systems
- Ease of Entry
- Borderless
- Rapidly evolving
- AI-Enabled Attacks
- Everything is Connected
- Internet of Things (IoT) Proliferation

UNCLASSIFIED

Courtesy graphic by MITRE

Integrating a Threat-Informed Framework

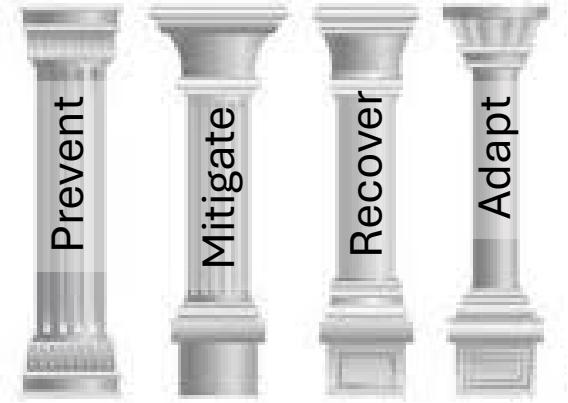
- DoW has published substantial policy, doctrine and engineering documentation to assist in guiding the development and fielding of secure IT and computing systems
  - DoW embracing zero trust as the primary framework for ensuring protection against emerging threats

- Typical cyber protection and mitigation approaches (including zero trust) require adjustments due to unique physical access and environmental characteristics of Space Vehicles

Implementation of a **threat-informed framework** integrating new technological defenses is **essential** for all new spacecraft to ensure space-based warfighter operations through contested cyberspace

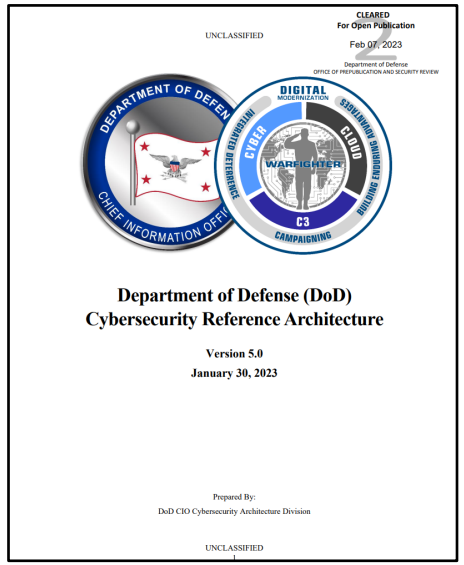
Key DoW Cybersecurity Reference Architectures & Frameworks

CJCS Cyber Survivability Endorsement (CSE)



- CSA 01 - Control Access (not RMF Access Control)
- CSA 02 - Reduce Cyber Detectability
- CSA 03 - Secure Transmissions and Communications
- CSA 04 - Protect Information from Exploitation
- CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels
- CSA 06 - Minimize and Harden Cyber Attack Surfaces
- CSA 07 - Baseline & Monitor Systems, and Detect Anomalies
- CSA 08 - Manage System Performance and Enable Cyberspace Defense
- CSA 09 - Recover System Capabilities
- CSA 10 - Actively Manage System's Config. to Achieve and Sustain an Operationally Relevant Cyber Risk Posture

DoD Cybersecurity Reference Architecture (CSRA)


UNCLASSIFIED

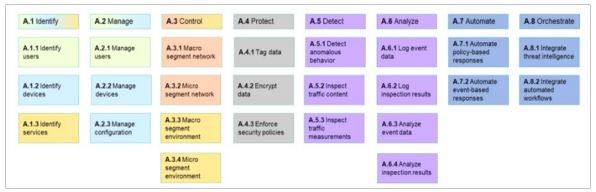
CLEARED
For Open Publication
Feb 07, 2023
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DoD)
Cybersecurity Reference Architecture

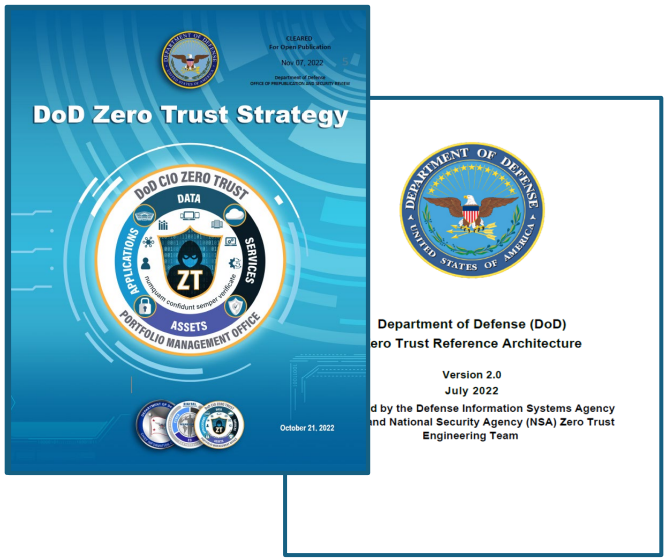
Version 5.0
January 30, 2023

Prepared By:
DoD CIO Cybersecurity Architecture Division

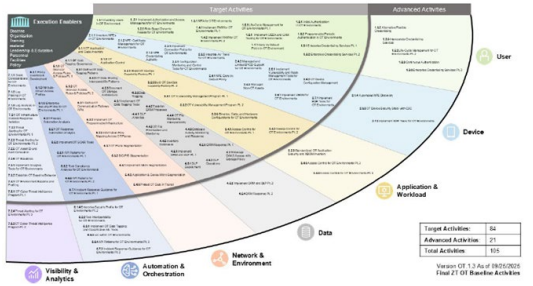
UNCLASSIFIED



DoD Zero Trust RA & Strategy



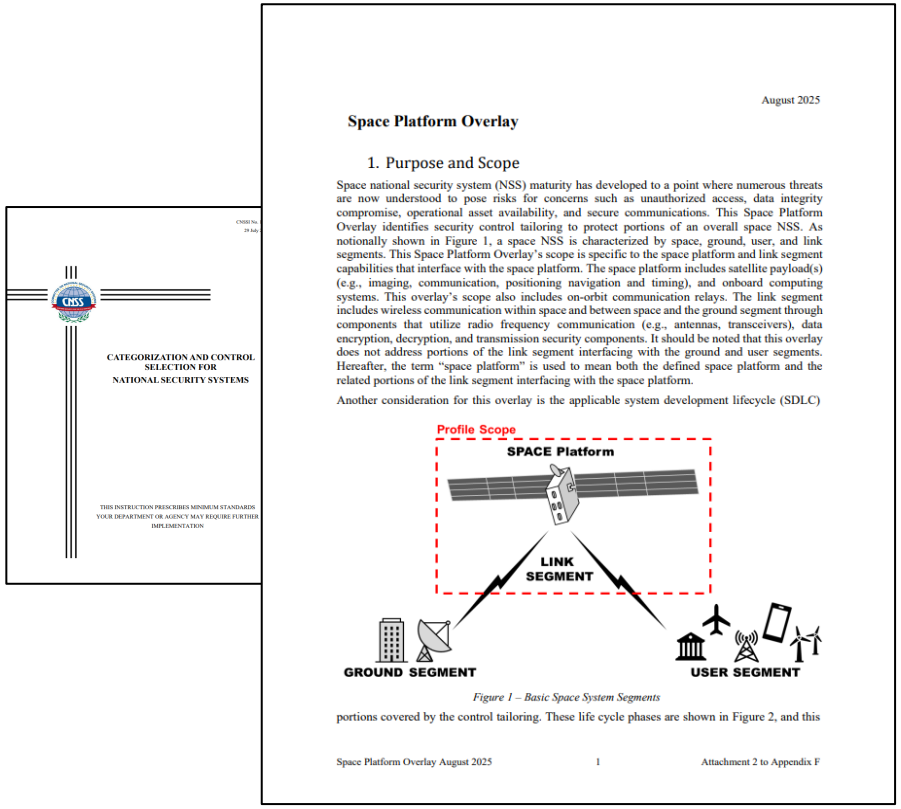
Zero Trust Fan Chart for Operational Technologies



These references are key to build a threat informed framework, but are not tailored for the Space Environment

CNSSI 1253 Appendix F - Attachment 2 (Space Platform Overlay)

- The official set of tailored cybersecurity requirements for U.S. National Security Systems (NSS) operating in space
  - It modifies the standard CNSSI 1253 controls to create a realistic and effective baseline specifically for the space platform and its associated link segments (e.g., space-to-ground communication).
  - The Space Overlay tailors controls based on several core assumptions about the operational environment



CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS

THIS INSTRUCTION PRESCRIBES MINIMUM STANDARDS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION

August 2025

Space Platform Overlay

1. Purpose and Scope

Space national security system (NSS) maturity has developed to a point where numerous threats are now understood to pose risks for concerns such as unauthorized access, data integrity compromise, operational asset availability, and secure communications. This Space Platform Overlay identifies security control tailoring to protect portions of an overall space NSS. As notionally shown in Figure 1, a space NSS is characterized by space, ground, user, and link segments. This Space Platform Overlay's scope is specific to the space platform and link segment capabilities that interface with the space platform. The space platform includes satellite payload(s) (e.g., imaging, communication, positioning navigation and timing), and onboard computing systems. This overlay's scope also includes on-orbit communication relays. The link segment includes wireless communication within space and between space and the ground segment through components that utilize radio frequency communication (e.g., antennas, transceivers), data encryption, decryption, and transmission security components. It should be noted that this overlay does not address portions of the link segment interfacing with the ground and user segments. Hereafter, the term "space platform" is used to mean both the defined space platform and the related portions of the link segment interfacing with the space platform.

Another consideration for this overlay is the applicable system development lifecycle (SDLC)

Figure 1 – Basic Space System Segments

portions covered by the control tailoring. These life cycle phases are shown in Figure 2, and this

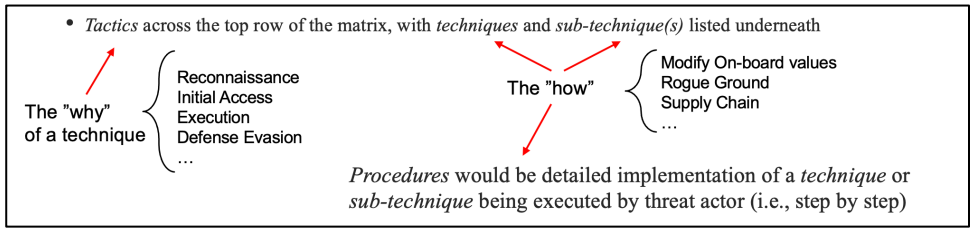
Space Platform Overlay August 2025 1 Attachment 2 to Appendix F

CNSSI 1253 AppF Att2: Space Platform Overlay

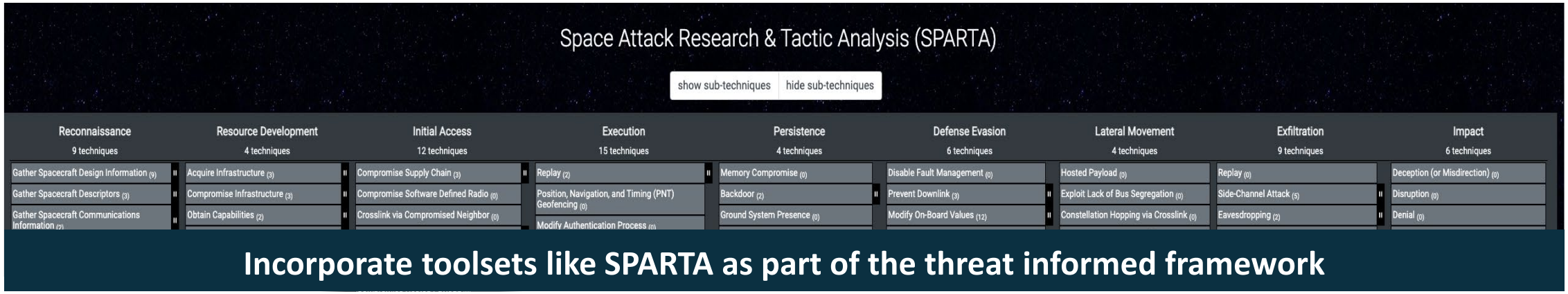
For a threat informed framework, security controls alone aren't enough

Space Attack Research & Tactic Analysis (SPARTA)

- Cybersecurity matrices are industry-standard tools and approaches for commercial and government users to navigate rapidly evolving cyber threats and vulnerabilities and outpace cyber threats
  - They provide a critical knowledge base of adversary behaviors
  - Framework for adversarial actions across the attack lifecycle with applicable countermeasures



- Aerospace's SPARTA matrix is the first-of-its-kind body of knowledge on cybersecurity protections for spacecraft and space systems, filling a critical vulnerability gap for the U.S. space enterprise. Promotes threat informed (i.e., Techniques, Tactics, and Procedures (TTPs)) defense-in-depth

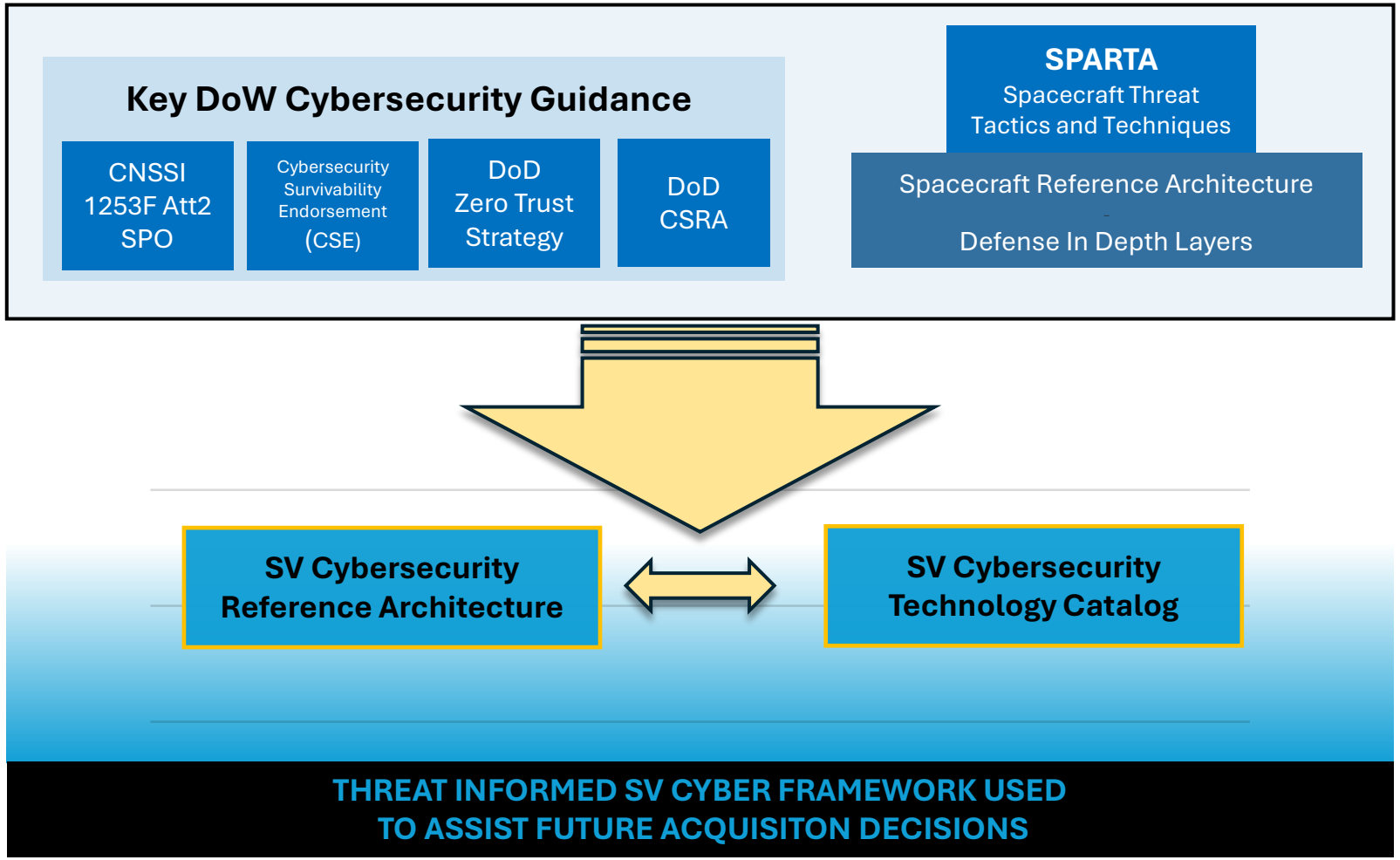


Incorporate toolsets like SPARTA as part of the threat informed framework

Threat Informed Framework – Emerging Products

Objectives

- Amend existing directives and guidance with SV-specific, implementable guidance and direction to streamline acquisitions and integration of advanced cyberspace defense
- **Leverage threat models** to emphasize protection against the highest priority threats
- Highlight existing technology and gaps to **optimize investments** and reduce program Non-Reoccurring Engineering (NRE)
- **Streamline acquisitions and integration** of advanced cyberspace defense into space programs



Sample SV Cybersecurity Zero Trust Capability Set

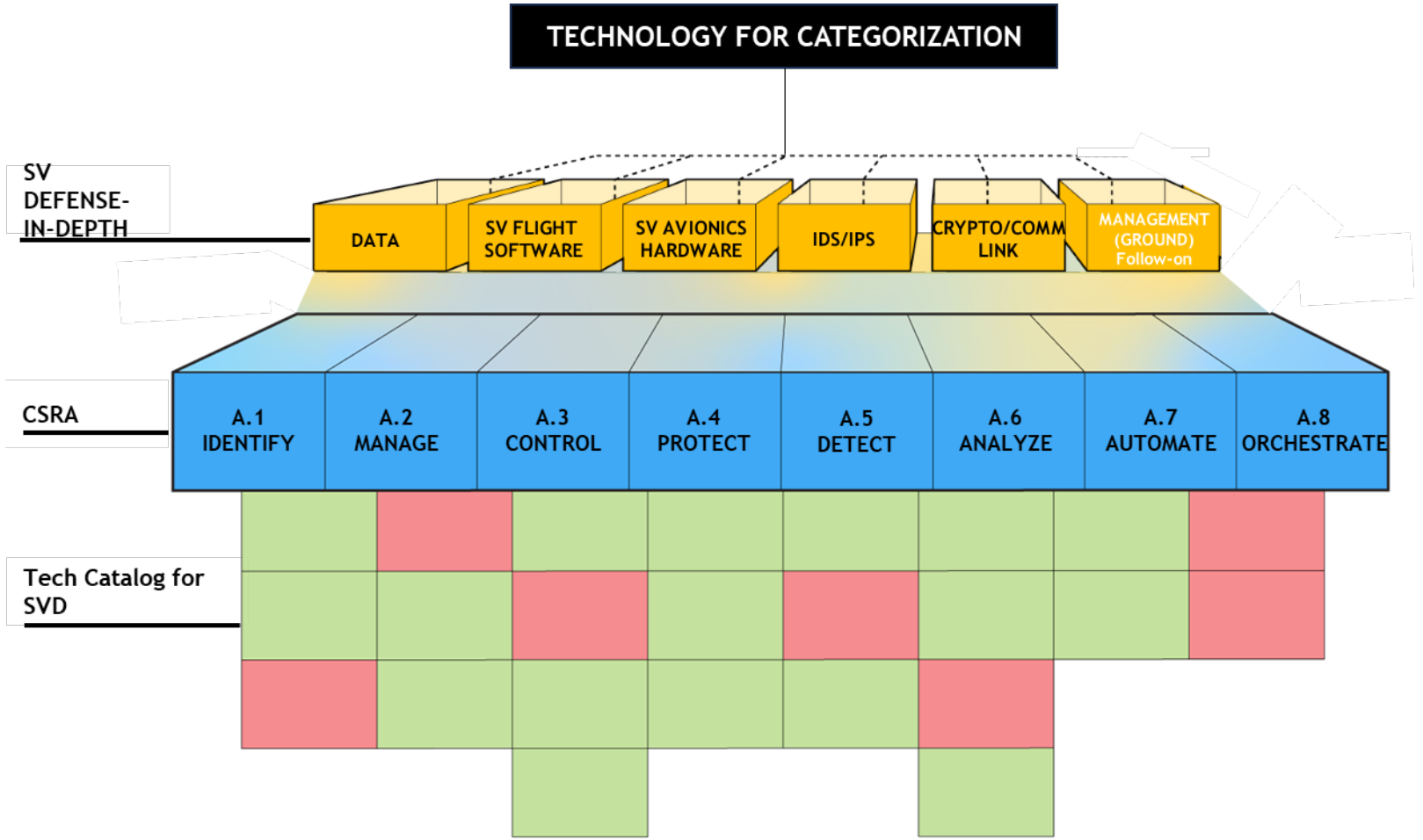
- Defines the security capabilities required within a Space Vehicle to achieve Zero Trust outcomes and ensure mission assurance in a contested domain.
- Closely aligned with threat countermeasures, capabilities within the Reference Architecture (RA) will
  - Be allocated to specific portions of a spacecraft architecture, including defense-in-depth layer
  - Retain documented links to policy or requested stakeholder needs to support compliance assessment
  - Establish alignment against threat TTPs to provide a foundation for derived requirements and design guidance to be properly threat-informed and aligned

IDENTITY	DEVICES	NETWORKS	APPLICATIONS & WORKLOADS	DATA	VISIBILITY & ANALYTICS	AUTOMATION & ORCHESTRATION
ID-01: Identity Provisioning/ Credentials	**DV-01:** Trust Anchors (Hardware or Software)	**NW-01:** Network Access Control & Authentication for All Links	**AW-01:** Workload Identity & Signature Verification	**DT-01:** Data Classification, Labeling & Metadata Binding	**VA-01:** Telemetry & Event Collection Framework	**AO-01:** Policy-Driven Autonomous Decision Engine
ID-02: Mutual Authentication (Ground <> Space <> Crosslink <> Subsystem)	**DV-02:** Secure Boot & Boot-Time Verification	**NW-02:** Network Segmentation & Micro-Segmentation	**AW-02:** Secure Execution Environment & Isolation Domains	**DT-02:** Data Encryption & Integrity Protection (At Rest, In Transit, In Use)	**VA-02:** Distributed Logging & Tamper-Evident Storage	**AO-02:** Cross-Domain Orchestration
ID-03: Session Management & Identity-Aware Command Execution	**DV-03:** Firmware & Configuration Integrity Protection	**NW-03:** Secure Routing, Switching & Path Validation	**AW-03:** Least-Privilege Enforcement & Capability-Based Access Control	**DT-03:** Data Access Control & Least-Privilege Enforcement	**VA-03:** System-wide / Cross-domain Correlation & Analytics Engine	**AO-03:** Automated Response & Containment Mechanisms
ID-04: Authorization & Privilege Control (RBAC/ABAC/MBAC)	**DV-04:** Runtime Integrity Monitoring & Attestation	**NW-04:** Network Encryption & Cryptographic Segmentation	**AW-04:** Runtime Integrity Monitoring & Continuous Attestation	**DT-04:** Data Provenance, Traceability & Chain-of-Custody	**VA-04:** Identity-bound Observability Data (telemetry, logs, etc.)	**AO-04:** Identity Aware Automation
ID-05: Identity-Bound Data Access & Data-Centric Security	**DV-05:** Device Identity & Cryptographic Binding	**NW-05:** Traffic Integrity, Timing & Freshness Validation	**AW-05:** Secure Update, Patch, & Deployment Mechanisms	**DT-05:** Secure Data Storage, Segmentation & Compartmentalization	**VA-05:** Data Labeling, Classification, & Policy Enforcement for Telemetry	**AO-05:** Context and Mission Aware Enforcement
ID-06: Identity Telemetry, Monitoring & Analytics	**DV-06:** Least-Privilege Hardware Access Control	**NW-06:** Network Telemetry, Monitoring & Analytics	**AW-06:** Data-Centric Protection Within Applications	**DT-06:** Data Lifecycle Governance (Retention, Sanitization, Deletion)	**VA-06:** Autonomous Detection & Onboard Response	**AO-06:** Secure Workflow & Playbook Management
ID-07: Intra-System Identity Validation (Internal Bus Enforcement)	**DV-07:** Hardware Interface Protection & Access Enforcement	**NW-07:** Network Configuration Integrity & Attestation	**AW-07:** Application Behavior Monitoring, Telemetry Correlation, & Anomaly Detection	**DT-07:** Data Audit Logging, Monitoring & Anomaly Detection	**VA-07:** End-to-End Audit Fabric & Forensic Reconstruction	**AO-07:** Autonomous ZPolicy Distribution & Synchronization
ID-08: State, Mode, and Session Aware Identity Enforcement (e.g., dynamic)	**DV-08:** Data Protection on Devices (At Rest & In Transit)	**NW-08:** Dynamic Re-Keying & Cryptographic Session Management	**AW-08:** Comprehensive Audit Logging & Onboard Policy Enforcement		**VA-08:** Ground to Space to Crosslink Observability Integration	**AO-08:** Closed-Loop Detection, Decision, Enforcement Integration
ID-09: On-Orbit Credential & Key Lifecycle Management	**DV-09:** Device Logging, Telemetry & Trust Analytics	**NW-09:** Network Logging & Audit			**VA-09:** Model & Rule Validation for AI/ML Analytics	**AO-09:** Event Provenance, Audit, and Traceability for Autonomous Actions
	DV-10: Device-Level Fault Containment & Autonomous Recovery					**AO-10:** Safety-Guarded Automation & Fail-Safe Controls

NOTIONAL CAPABILITIES SET

Identify Zero Trust capability areas for space vehicles by associating threat to defensive measures

SV Cyber Technology Catalog Framework



This framework organizes SV cybersecurity technologies using:

1. SV Defense-in-Depth Layers (where technology is implemented)
2. DoD CSRA Activities (what security functions it provides)

The result is a populated technology catalog that enables programs to:

- **Identify technology gaps** (Red)
- **Accelerate Acquisition of Mature Solutions** (Green)

DoD CIO Reference Architecture

CSRA Activities and Sub-Activities

A.1 Identify	A.2 Manage	A.3 Control	A.4 Protect	A.5 Detect	A.6 Analyze	A.7 Automate	A.8 Orchestrate
A.1.1 Identify users	A.2.1 Manage users	A.3.1 Macro segment network	A.4.1 Tag data	A.5.1 Detect anomalous behavior	A.6.1 Log event data	A.7.1 Automate policy-based responses	A.8.1 Integrate threat intelligence
A.1.2 Identify devices	A.2.2 Manage devices	A.3.2 Micro segment network	A.4.2 Encrypt data	A.5.2 Inspect traffic content	A.6.2 Log inspection results	A.7.2 Automate event-based responses	A.8.2 Integrate automated workflows
A.1.3 Identify services	A.2.3 Manage configuration	A.3.3 Macro segment environment	A.4.3 Enforce security policies	A.5.3 Inspect traffic measurements	A.6.3 Analyze event data		
		A.3.4 Micro segment environment			A.6.4 Analyze inspection results		

- Note: Not all activities will make sense to do at each defense-in-depth layer

- Ref: DoD CIO Reference Architecture: https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

THANK YOU!

SATELLITE CYBERSECURITY: MULTI-LAYER DEFENSE IN DEPTH STRATEGY

SATELLITE SUBSYSTEMS

ONBOARD COMPUTER (OBC/)
- Processor
- Memory
- Flight Software

COMMUNICATIONS (TT&C)
- Antennas
- Transceivers
- Encryptors

ATTITUDE & ORBIT CONTROL (AOCS)
- CNC Computer
- Cyros
- Star Trackers
- Reaction Wheels

ELECTRICAL POWER (EPS)
- Solar Panels
- Batteries
- PMAD

PROPULSION
- Thrusters
- Fuel
- Tanks, Valves

PAYLOAD
- E.g., High-Res Camera
- Science Instrument

ATTACK VECTORS & VULNERABILITIES

Command Injection & Control Hijacking:
(Injecting rogue commands to alter orbit, turn off systems, or take full control)

Legacy Software, Hardware & Crypto:
(Can't be patched on orbit)

Ground Segment Exploitation:
(Hacking ground stations to access and control the space asset)

Supply Chain Vulnerabilities:
(Compromised hardware or software during build and assembly)

Data Interception & Eavesdropping:
(Capturing unencrypted commands and payload data)

DDoS on Space Links:
(Overwhelming comms links with fake requests, causing denial of service)

DEFENSE MEASURES ON THE SATELLITE

SECURE BOOT & FIRMWARE
Validates genuine software

AUTHENTICATION & ACCESS CONTROL
Only authorized users

ENCRYPTION (AES-256)
Protects commands, telemetry, and payload data

INTRUSION DETECTION (HIDS)
(Deep-packet and log monitoring)

STRONG AUTHENTICATION & ACCESS CONTROL
(MFA for all interfaces)

CYBER DATA TO SEND TO GROUND (TELEMETRY)

ZERO TRUST PRINCIPLES
(Never trust, always verify internal component data)

OBC BEHAVIORAL ANALYSIS
(Detects unusual process execution)

DYNAMIC RESPONSE POLICIES
(e.g., enter safe mode on multi-layer alert)

SECURE DOWNLINK

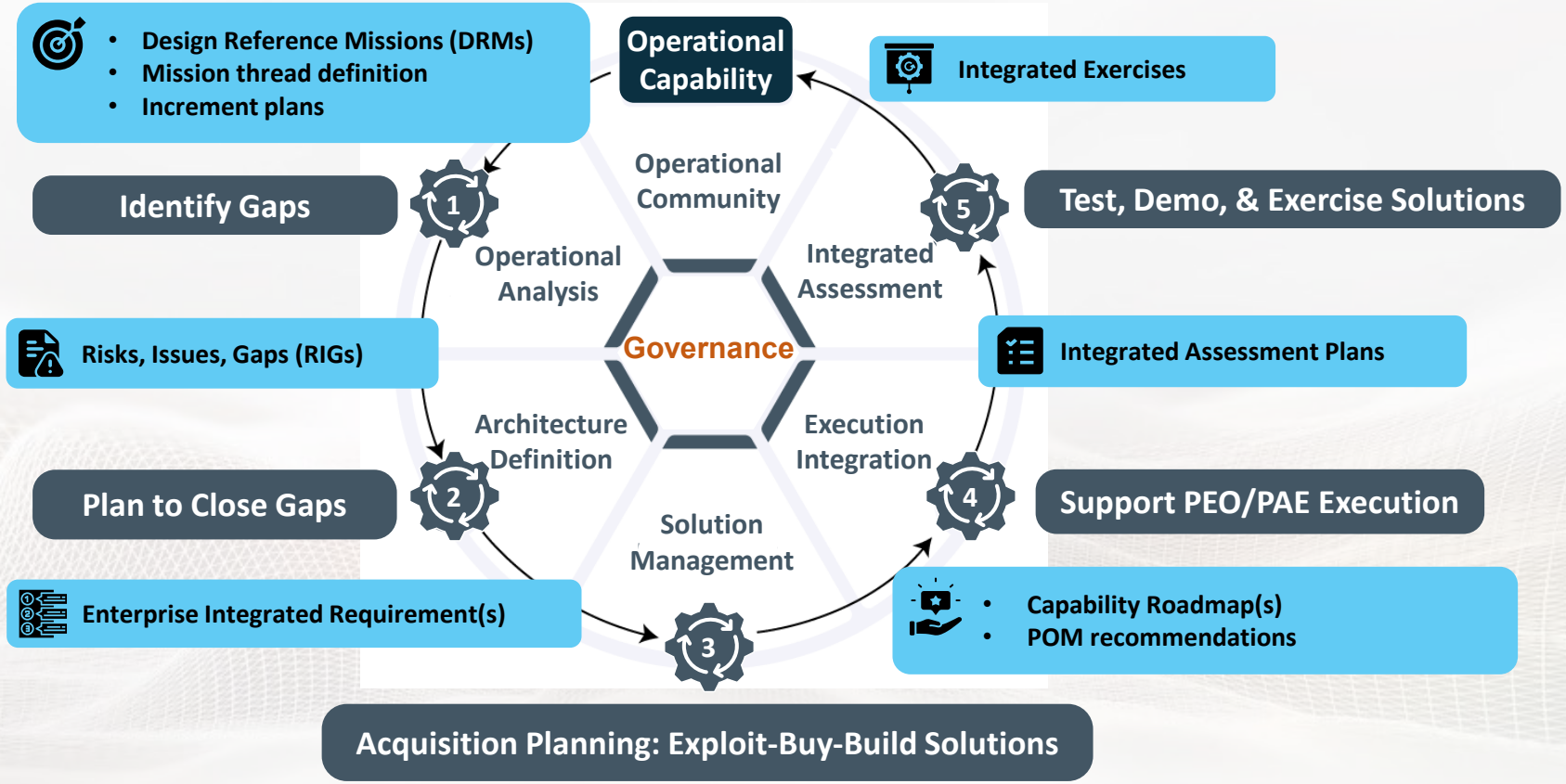
GROUND OPERATIONS CENTER (GOC)

System of Systems Engineering (SoSE) for Integration

START: Mission threads with defined parameters (Joint Operational Plans)

Warfighter Need

FINISH: Fully burdened, integrated systems that perform mission



Rigorous, robust, & repeatable process to produce integration artifacts for enforced governance

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

Maturing Space Sensing through Digital Engineering

Mr. Mario Goins, Systems Engineer
Mr. Douglas Brown, Requirements & Integration Chief
SSC Space Sensing Program Executive Office

Cyber Readiness at the Speed of Space

Agenda

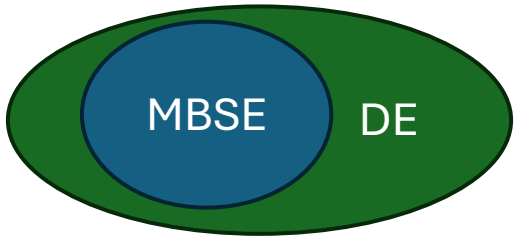
- Primer of MBSE/DE
- Benefits of DE Maturity
- Research from 2025/2026
- SYD 84/S5 Maturity Model/Future Plans
- Questions/Comments

MBSE & DE Primer

MBSE (Model Based Systems Engineering)

- **Systems Engineering** using models instead of documents
- Architectural (low-medium fidelity) models (ie, Cameo, Rhapsody, etc)
- High level simulation to answer systems engineering questions
  - What requirements are impacted by a system architecture change?
  - If program X implements an interface design change, what other programs across the portfolio are impacted?
  - If program X's system performance fails to meet requirements, what other programs across the portfolio are impacted
  - Useful as a planning tool

DE (Digital Engineering)



- **System Design** using models
- Component (high fidelity) models
- Digital Twin (DT) emulates a perfect Engineering Model
- Low level, physics-based models & simulations
  - How well does a component perform under expected thermal, vibration, radiation, aging, operational, stress, and denied conditions?
  - What's the max throughput of this network design for the required messages?
  - How well does this optical focal plane design withstand directed energy attacks?
  - DE/Digital Twin tool commercial examples:
    - Comms: OPNET/Riverbed, Qualnet/EXata/Keysight
    - Physics: Fluent, Twin Builder, ClockFX, MATLAB/Simulink

Benefits of DE Maturity

Objective:

Use research to simplify DE integration within SN/SYD84 and help consolidate and to simplify DE Approaches/Standards.

Benefits for SYD 84:

- Increase DE Efficiency & Productivity
- Enhance DE Collaboration
- Faster DE Innovation & Testing
- Improve DE Quality & Reduce Risk for Acquisition

Research for MBSE/DE

SYD84/S5 DE Maturity Study

SYD84/S5 DE Maturity Study

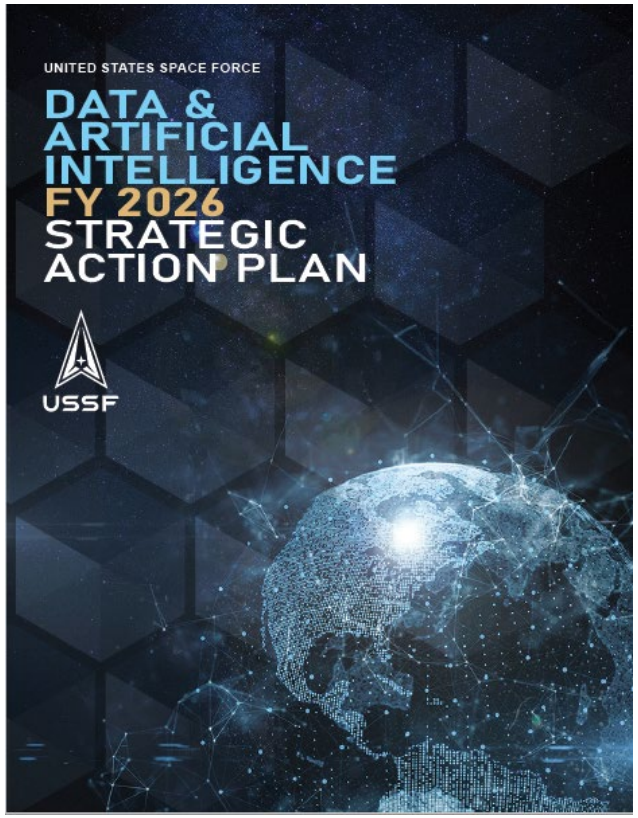
Progress/Timeline:

Q2- Q4 2025:

- Research conducted with government and industry Digital Engineering SMEs (BAH, MITRE, Cadence, Navy and RAND)
- Reviewed DTO and CDAO Data and AI Guidelines and Standards (2025)
- Reviewed USSF Data and AI Strategic Action Plan (2025)
- Created DE Maturity Model (Q4 2025)
- SYD 84 Leadership Support for DE Maturity Survey

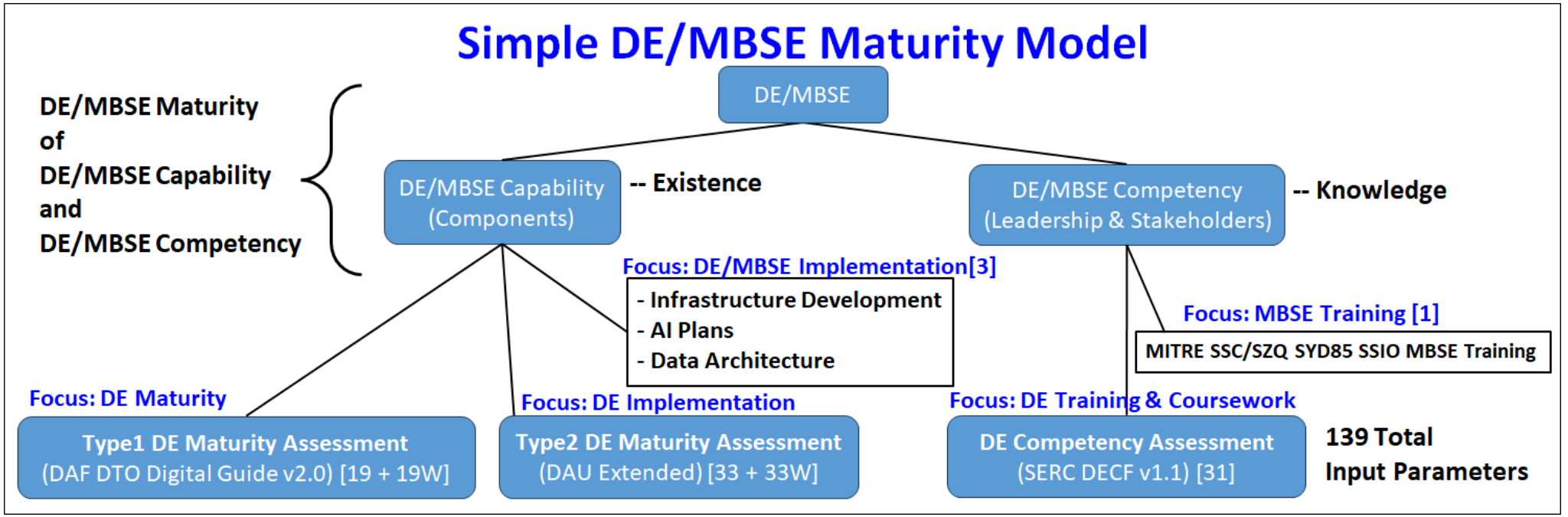
Q1 -Q3 2026:

- SYD 84 TMT Tasker for DE Maturity Survey (MG, MW, MT programs)
- Reviewed Q1 2026 USSF Data and AI Action Plan
- Researching solutions for Metadata Tagging
- Data Review of DE Maturity Survey



DE Maturity Model

- **DE/MBSE Maturity Model (Capability, Competency)**
  - **DE Capability (Components) and Competency (Training)**



Maturity

Interoperability [2]
ASOT [2], MBSE [2]

Implementation

DEE [2]*, Software with ATOs [2]*
Stakeholder Models: Architecture [2]*
Methodology: Tools [2]*
Infrastructure Dev, AI Plans, Data Architecture [3]
*4 weights ignored

Competency

Data Mgmt, Modeling, Simulation, AI/ML, Data Analytics, Digital Arch, Digital Model Based Review, Configuration Mgmt, Dig. Literacy [9]

54

SYD 84/S5 Future DE Tracking

Concurrent Infrastructure Developments

USSF CTIO Digital Services Ecosystem (DSE)
Req1: Data Federation
Req2: User Interface
Req3: Governance
Req4: Security
Req5: Technology
CTIO -- Chief Technology & Innovation Office

Data Strategy

- **Enterprise API Gateway (Fast data)**
- **Data Mesh Env. (Federated data)**
- **Data Domain (platforms)**
- **ADS (Authoritative Data Source)**
- **Sensors**

Both methods can lead to an optional Digital Twin Development, while maturation across Data and AI standards is implemented. Leads to options of additional pathways of the DE Maturity Model(Capability).

Ongoing independent infrastructure development (DSE, CDAO)

Missile Track Digital Engineering Applications

Background:

- SYD 84 has completely moved to digital engineering (e.g., upfront architecture analysis, source selection, all technical milestone reviews, etc.) for MEO Epoch 2 and beyond on Spacestation
- Contractors have been provided Government Acquisition Model with PWS, SOW, Reference Material & SETR criteria
- Contractors are developing solutions that conform with direct traceability in a Solutions Template (Model-based RFP response)

Digital Engineering Examples:

- Supports senior leader decision-making – contractor validated requirements with homogenous proprietary constellation
- Supporting program requirements V&V with MBSE model – Developing digital twins of GMI & FORGE ground systems to simulate interactions
- Lifecycle Management – All technical reviews performed with MBSE model
- Enterprise SOSI – Interfaces native to Government Reference Architecture

Future Initiatives:

- Digital twin factory flat-sats (engineering development units) for end-to-end test
- Digital “Hardware in the Loop” emulators

SYD 84 to formalize DE approach with MT best practices to stay in sync with external USG orgs & industry

Conclusion

Future Plans:

Metadata Tagging (Start Q3)

- Proper metadata tagging improves searchability and data governance, better enables data discovery and reuse.(Acquisition)

Skills Development

- Keeps workforce up to date on the knowledge curve and how to efficiently and securely utilize data.

Authoritative Source of Truth (ASoT)

- An ASoT lets programs better ensure data quality & consistency.

Formalized SYD 84 DE Strategy

- Coalescing higher headquarters guidance and MEO Missile Track best practices to create a formal SYD 84 DE strategy

Questions?

2026 SSC CYBER EXPO

Mission Application of Continuum and Quantum Computing

Mr. Surya Singh, PNNL Cyber Engineer

Dr. Duncan Earl, Director Quantum Networking at IonQ

Cyber Readiness at the Speed of Space

2026 SSC CYBER EXPO

A Vision for Continuum Computing for Space

Mr. Surya Singh, PNNL Cyber Engineer

Cyber Readiness at the Speed of Space

Continuum Computing for Space: Overview

- Continuum Computing for Space is an architectural and operational paradigm that integrates onboard/edge compute (spacecraft), ground edge (ground stations), on-prem mission HPC, and commercial cloud into a seamless environment for dynamic workload orchestration, real-time data processing, and elastic resource allocation across the end-to-end space enterprise
- Thesis: Provide a mission-aware continuum computing architecture that seamlessly integrates space, ground, cloud, and edge environments that enable the USSF/SSC to achieve resilient, secure, and real-time operations, delivering decision advantage in contested, multi-domain environments.

Dynamic Solutions to SSC Challenges

SSC Challenges and CC for Space Solutions:

- Siloed ground and mission systems -> Enable platform a unifying digital layer/Unified cloud, Edge, and HPC environment
- Delayed software updates to space systems -> Enable continuous software delivery to ground systems and satellites
- Data latency across domains -> Enable Edge +AI to process data where generated
- Cyber security and supply chain risks -> Enable continuous assurance through policy-as-code security

Why Space Missions Need a Continuum

- Traditional approaches force a choice between performance, flexibility, and accessibility; CC for Space removes that tradeoff by enabling workloads to move/scale across environments
- Space Drivers
  - Intermittent connectivity, constrained downlink, variable latency
  - Data volume growth (EO, RF sensing, hyperspectral, SAR-like payloads)
  - Need for autonomy and faster “sensor-to-insight” timelines
  - Mission assurance: safety, cyber, supply chain, and compliance constraints

Space Continuum Execution Environments

- Space Edge (Onboard): payload processors, flight computers, rad-tolerant accelerators
- Ground Edge: processing at/near antennas for rapid ingest, triage, first-look products
- Mission On-Prem/HPC: high-end processing, fusion, large-scale simulation/digital twins
- Commercial/Gov Cloud: elastic analytics, collaboration, distribution, long-term storage

Principle: place computation where it best meets latency, bandwidth, cost, and security needs

Core Definitions

- Edge Computing: computation close to the data source (spacecraft sensors or ground-station ingest), enabling low-latency processing, reduced data movement, and operation in disconnected/bandwidth-constrained conditions
- Elastic Compute: dynamically scaling CPU/GPU/memory/storage across environments to match changing mission demands (e.g., surge processing during a contact window)
- AI-Driven Orchestration: automated decisions on where/how workloads run, factoring performance, cost, security, data gravity, and real-time system health

Continuum Computing Conceptual Model

Mission Governance Layer

”The decision layer that aligns continuum operations with strategy, compliance, cost, and mission priorities.”

Common Services (X-Platform) Layer

“Standardized tools and services that unify how users develop, run, and observe workloads across the continuum.”

Continuum Control Layer

"The coordination engine that intelligently routes workloads, enforces policies, and connects platforms into a unified computing fabric."

Platform Layer (Cloud, HPC, Edge

“Diverse execution environments that power the full range of scientific computing workloads.”

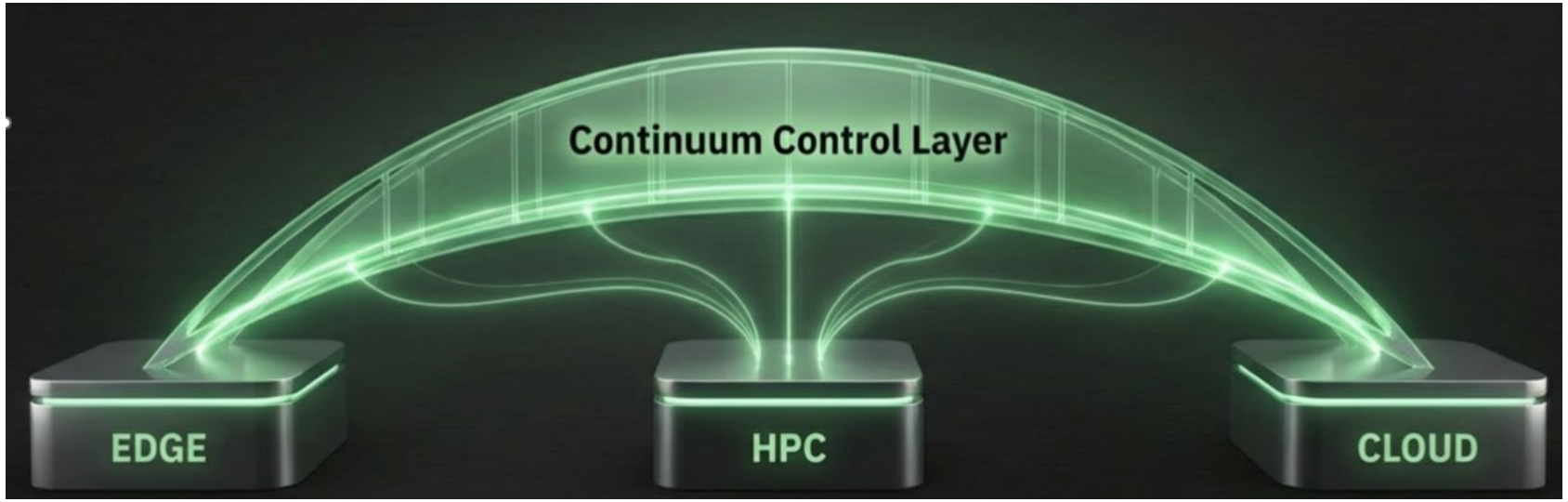
Mission Governance Layer: Space-Specific Controls

- Policy & Compliance: export controls, data rights, spectrum constraints, safety-of-flight rules
- Cost & Resource Management: downlink allocation, onboard power/thermal budgets, cloud spend
- Security & Trust: zero-trust identity, key management for spacecraft/ground, supply-chain assurance
- Outcome: consistent mission rules regardless of where code runs.

Common Services (X-Platform) for Space Missions

- DevSecOps pipeline: reproducible builds, signed artifacts, staged rollout, rollback
- Observability: unified telemetry/logs/metrics across spacecraft + ground + cloud
- Data services: catalog/metadata, provenance, access control, policy enforcement
- Model lifecycle: train (HPC/cloud), validate, package, deploy to edge, monitor drift

Continuum Control Layer: Orchestration & Routing



Space-adapted capabilities:

- Contact-aware scheduling: run heavy tasks when downlink/contact exists; defer/queue otherwise
- Policy-based placement: keep sensitive processing on-prem; burst overflow to cloud (“cloudbursting” concept)
- Health-aware failover: switch to alternate ground edge or cloud region if degraded
- Data-gravity aware routing: process near where data is produced/stored to reduce movement

Computational Platform Layer

The intelligent connective tissue of the Continuum that enables high-performance, policy-aware data and workload movement between Cloud, HPC, and Edge environments. It ensures that compute, storage, and analytics operate as one integrated digital fabric.

Capability Descriptions	
High-Performance Connectivity	Provides low-latency, high-bandwidth links (e.g., ESnet, Science DMZ, optical peering) to support distributed, data-intensive science.
Programmable Network Plane	Enables dynamic provisioning, segmentation, and policy-driven routing through software-defined networking (SDN) and network-as-code.
Data Path Optimization	Intelligently manages data movement across sites to minimize latency, cost, and congestion while maximizing throughput and reliability.
Network Resilience	Monitors and automatically recovers from disruptions, rerouting traffic and preserving workflow continuity.
Zero-Trust Enforcement	Embeds encryption, identity-based segmentation, and continuous validation of endpoints to ensure trust across federated domains.

Example End-to-End Flow (Sensor → Product → Distribution)

- **Onboard edge**: filter/compress, event detection, prioritize storage/downlink
- **Ground edge**: rapid ingest, first-look QA, low-latency alerting
- **On-prem/HPC**: batch reprocessing, multi-sensor fusion, large-scale calibration
- **Cloud**: elastic analytics, dissemination, collaboration portals/APIs
- **Governance + Control**: enforce who can run what/where, and when

Measuring Success / Readiness

Mission outcomes:

- Reduced time from collection → actionable product
- Lower downlink and storage pressure (less unnecessary data movement)
- Improved resilience during disconnects (edge-first operations)

Enterprise outcomes:

- Repeatable deployments (DevSecOps), consistent security posture
- Portable workloads across environments (less vendor/stack lock-in)
- Cost control via elastic compute + policy-based orchestration

Questions?

2026 SSC CYBER EXPO

Quantum Solutions

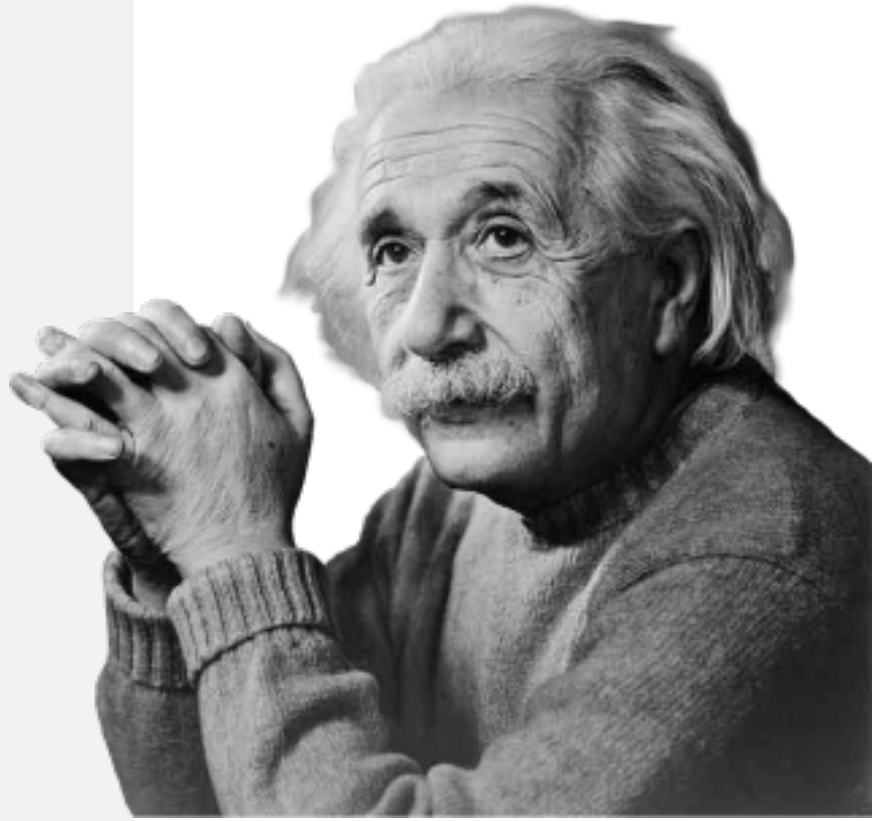
From Fiber to Orbit: The evolution of quantum networks

Dr. Duncan Earl, Director Quantum Networking at IonQ

Cyber Readiness at the Speed of Space

Agenda

- **What are quantum solutions?**
  - Quantum Computing
  - Quantum Sensing
  - Quantum Security
- **What are quantum networks?**
  - Fiber quantum networks
  - Satellite quantum networks
- **About IonQ**

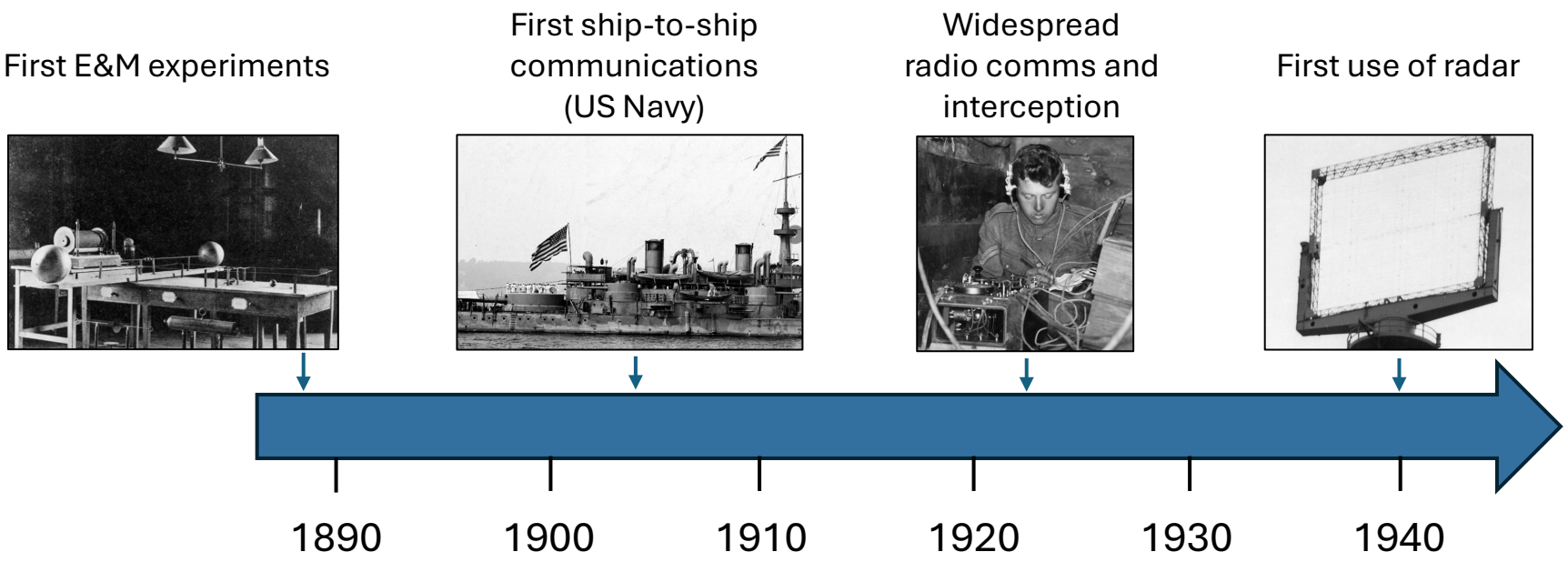


Quantum Solutions

New technology leveraging quantum physics

Emerging Technology

- **Past History: Electromagnetic (E&M) Waves**
  - Beginning in 1880's, newly understood E&M physics enabled powerful new military solutions

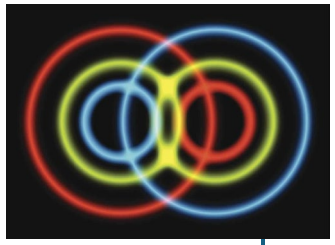


Radio Waves in the late 1800s were considered a scientific curiosity

Emerging Technology

- **Today: Quantum Waves**
  - Beginning in the 1980s, newly understood quantum physics begins enabling powerful new solutions

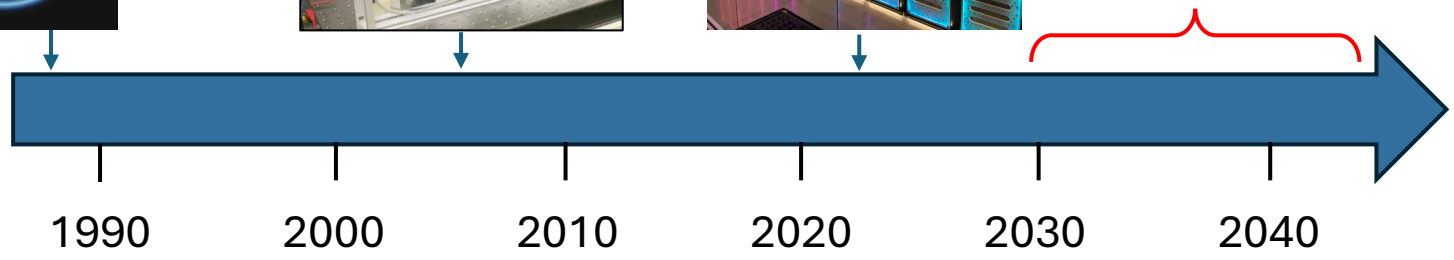
First Entanglement Generation Experiments



First deployment of quantum secure fiber communications

First commercial quantum network

- Powerful computers
- Precision global timing
- Secure GPS-free navigation
- Unbreakable crypto



Quantum technology is following that same trajectory

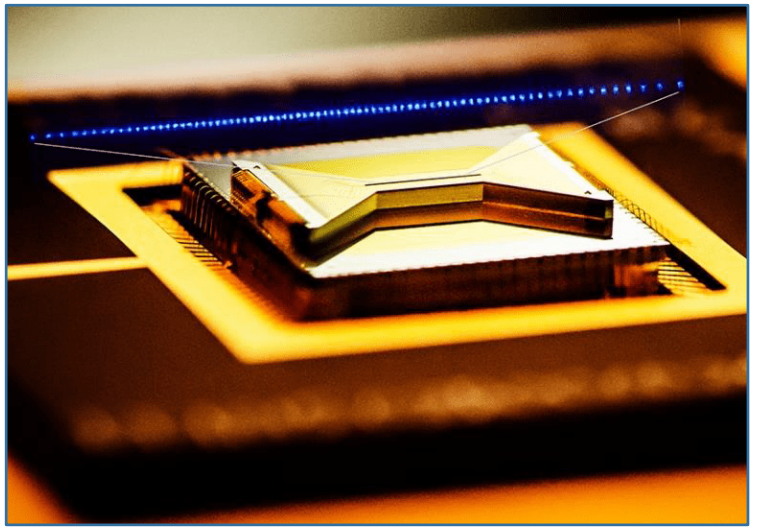
Quantum Computing

- **Quantum Computers** use *superposition* to create qubits existing in multiple states at once.
  - Enables new quantum computers that can solve problems impossible to solve with classical computers

Problems a quantum computer is expected to solve:

- Breaking today's encryption
- Room temperature superconductor materials
- Smaller, more powerful batteries
- Modeling complex chemistry
- Drug discovery for challenging diseases

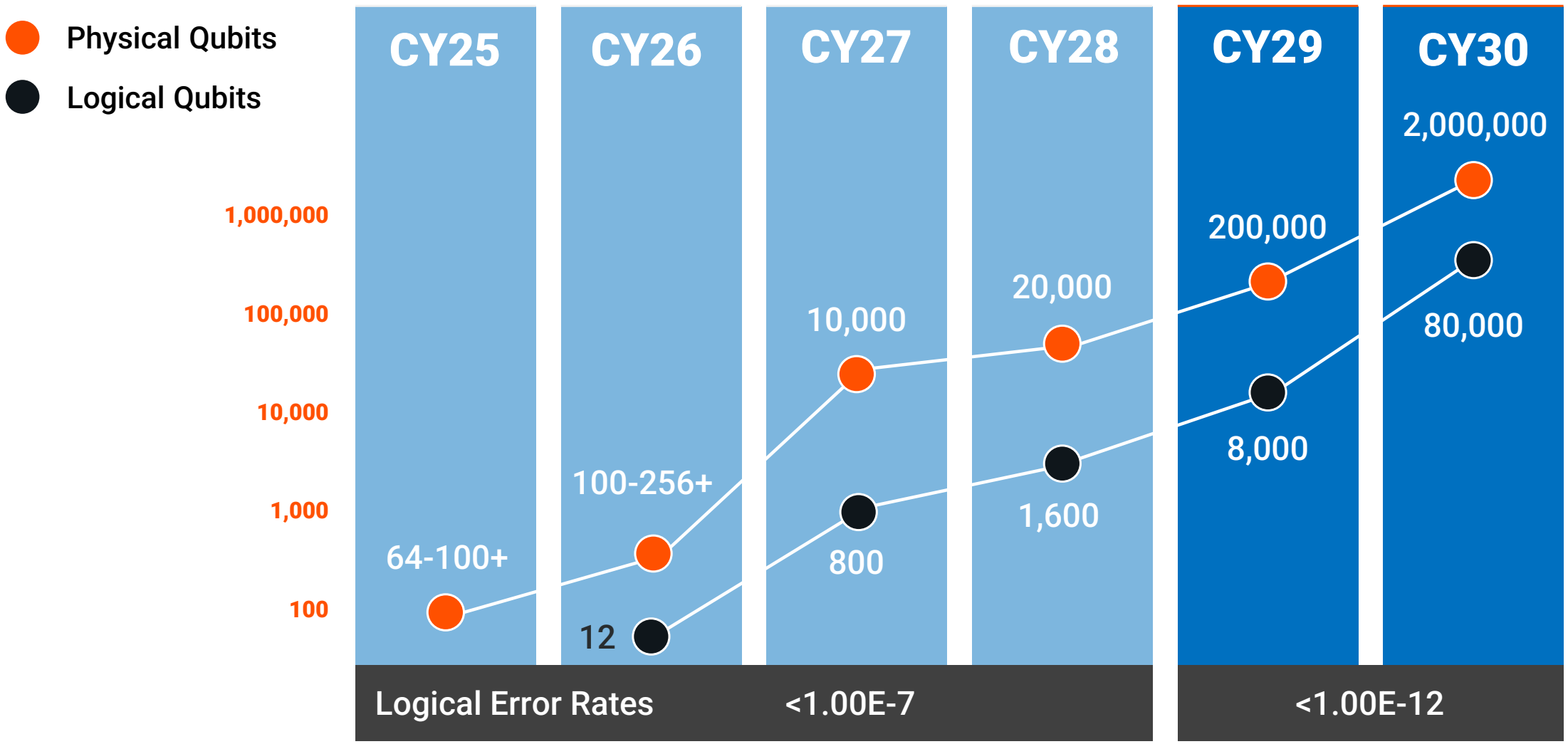
However, to solve these problems, we need to increase the number of quantum bits (qubits) in a quantum computer



Trapped Ion Quantum Computer (IonQ)

Powerful new computers based on quantum superposition

Qubit Growth



Quantum Sensing

- **Quantum Sensors use quantum physics to break the traditional limits on sensor noise and precision**
  - An individual quantum sensor improves performance, a network of these sensors even more so.

Better sensors using quantum:

- Ultra-precise atomic clocks
- Global picosecond timing synchronization
- Low-noise gravimeters, gyroscopes, & inertial sensors for GPS-free navigation
- Gravitational wave detectors

Atomic Clocks (IonQ)

Many of these solutions are commercialized today and ready for integration and use.

Powerful new sensors based on quantum physics

Quantum Security

- **Quantum cryptography** uses *quantum entanglement* to secure comms and stop eavesdropping

	Short Haul	Backbone	Long Haul	Hub & Spoke	Multiplex
					
Optical layer	Up to 60km (35mi)	60km – 100km (35mi – 62mi)	100km – 150km (62mi – 93mi)	Up to 90km (55mi)	Up to 60km* (37mi)
Optical layer	Shared Fiber Infrastructure (limited control on optical power distribution)				Owned Fiber
Optical layer	High Data throughout (i.e. >100Gbps)			Low to Medium Data throughput	
Operation Benefits	Easy hardware maintenance (independent Alice/Bob)		Optimized relay node	Optimized star Deployment**	Optimized optical fiber usage

Quantum Security

- **Quantum physics-based cryptography** that cannot be cracked by any computer (incl. quantum)

	Short Haul	Backbone	Long Haul	Hub & Spoke	Multiplex
					
Optical layer	Up to 60km (35mi)	60km – 100km (35mi – 62mi)	100km – 150km (62mi – 93mi)	Up to 90km (55mi)	Up to 60km* (37mi)
	Shared Fiber Infrastructure (limited control on optical power distribution)				Owned Fiber
	High Data throughout (i.e. >100Gbps)			Low to M	
Operation Benefits	Easy hardware maintenance (independent Alice/Bob)		Optimized relay node	Optimiz… Deployment	

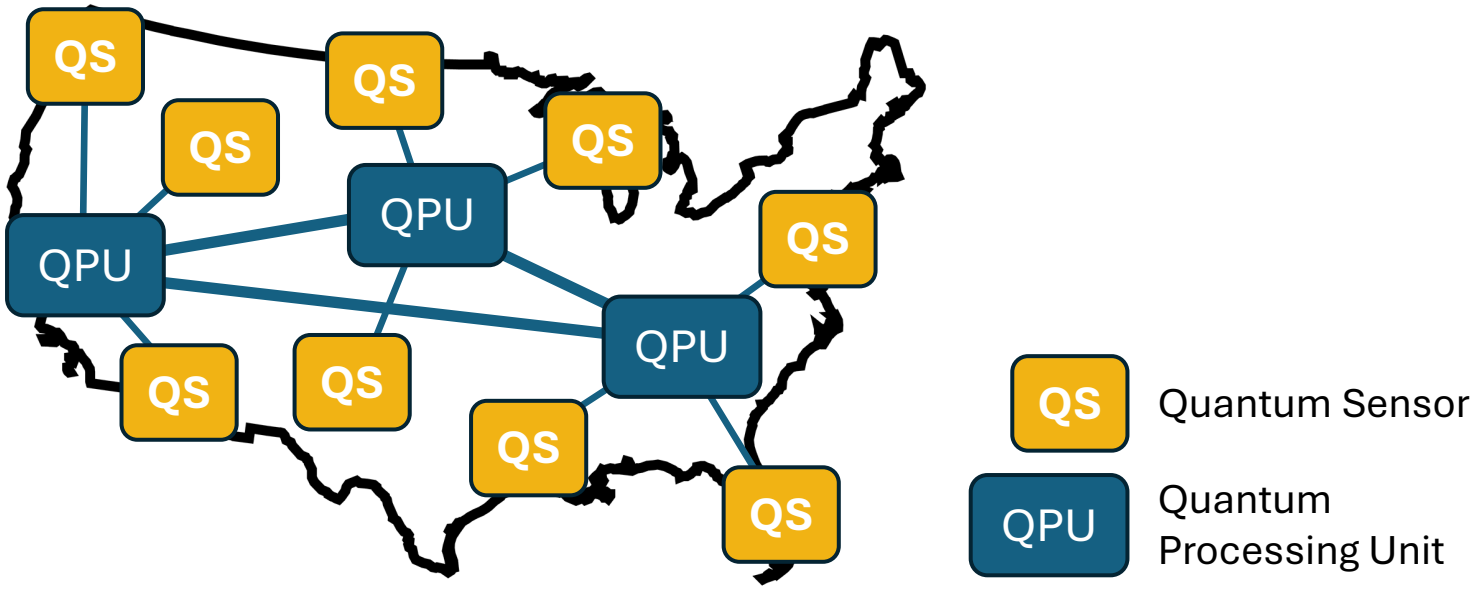
Ready for Q-Day!

Quantum Networks

Critical infrastructure
for quantum solutions

Quantum Networks

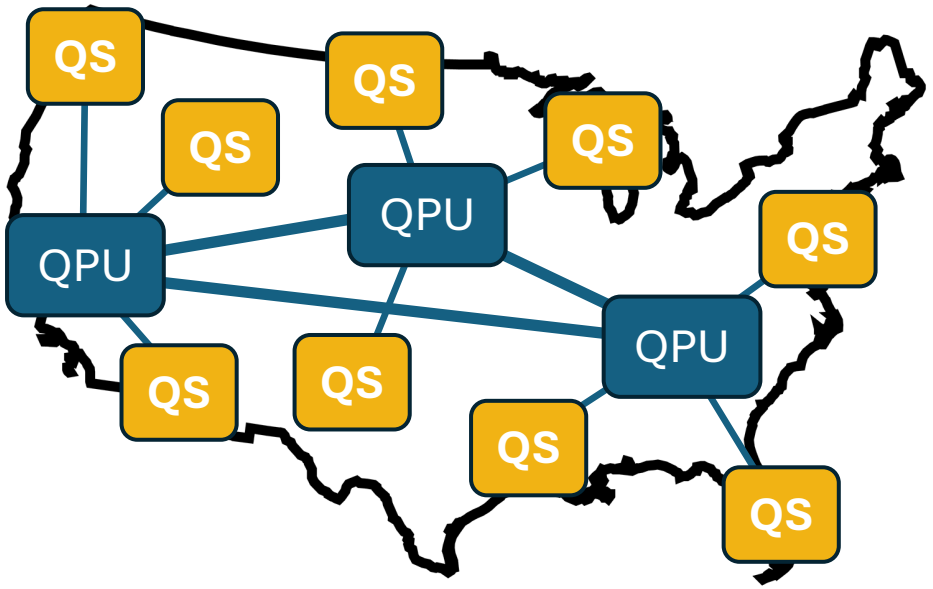
- **A quantum network is the infrastructure that links quantum devices together.**
  - Distributes entanglement to link devices so that they can operate coherently as a whole



Networks of quantum devices

Quantum Networks

- **A quantum network is the infrastructure that links quantum devices together.**
  - Distributes entanglement to link devices so that they can operate coherently as a whole



QS Quantum Sensor

QPU Quantum Processing Unit

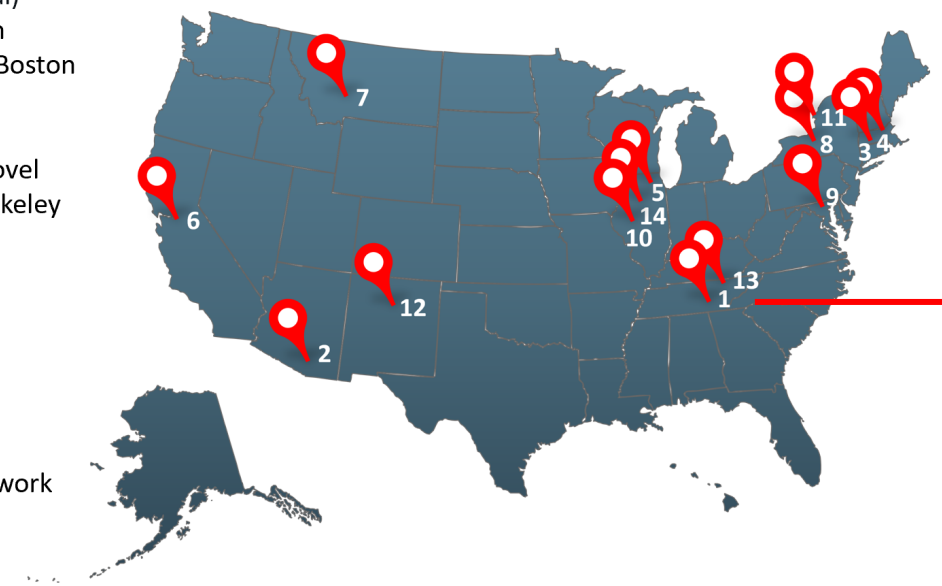
Distributed Quantum Sensing:
Egg Analogy

Networks of quantum devices

Quantum Network Status

- **Quantum network deployment began in the US around 5 years ago.**
  - Number of quantum networks is growing quickly and with increasing capabilities.

1. EPB Quantum Network (deployed/commercial)
2. Center for Quantum Networks (CQN) - Tucson
3. Boston-Area Quantum Network(BARQNET) - Boston
4. MIT Quantum Network Testbed - Boston
5. Chicago Quantum Exchange (CQE) - Chicago
6. Quantum Application Network Testbed for Novel Entanglement Technology (QUANT-NET) - Berkeley
7. MSU Quantum Network – Bozeman
8. AFRL Quantum Network – Rome
9. DC-QNet – Washington, DC
10. Hybrid Quantum Architectures and Networks (HQAN) – Urbana-Champaign
11. Tri-City Quantum Network – Sherbrooke
12. Los Alamos National Lab Quantum Network
13. Oak Ridge National Laboratory Quantum Network (Oak Ridge, TN)
14. Fermilab Illinois-Express Quantum Network



Commercial Quantum Data Center at EPB in Chattanooga, TN

Growth of Quantum Networks in the US

Network Progress

Terrestrial Quantum Networks

- Network links using optical fibers
  - Quantum entanglement over <25 km fiber is common today
  - Fiber distances >25km generally require quantum repeaters due to fiber loss
  - Quantum repeater technology advancing but still inefficient
  - Commercial terrestrial quantum networks are in operation in the US with subscribers

Space Quantum Networks

- Network links using satellites
  - Entanglement distribution between ground stations and satellites demonstrated (2017 – China)
  - Satellite-to-satellite entanglement expected to be demonstrated soon
  - It's an iterative process, progress being made
  - Has the potential to achieve very long entanglement distribution distances (>1000km).

Network Progress

Terrestrial Quantum Networks

- Network links using optical fibers
  - Quantum entanglement over <25 km fiber is common today
  - Fiber distances >25km generally require quantum repeaters due to fiber loss
  - Quantum repeater technology advancing but still inefficient
  - Commercial terrestrial quantum networks are in operation in the US with subscribers

Space Quantum Networks

- Network links using satellites
  - Entanglement distribution between ground stations and satellites demonstrated (2017 – China)
  - Satellite-to-satellite entanglement expected to be demonstrated soon
  - It's an iterative process, progress being made
  - Has the potential to achieve very long entanglement distribution distances (>1000km).

HYBRID

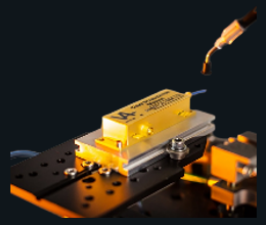
Long-Term Goal

About IonQ

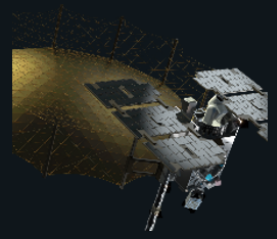
Pioneering tomorrow's quantum solutions

The IonQ Platform

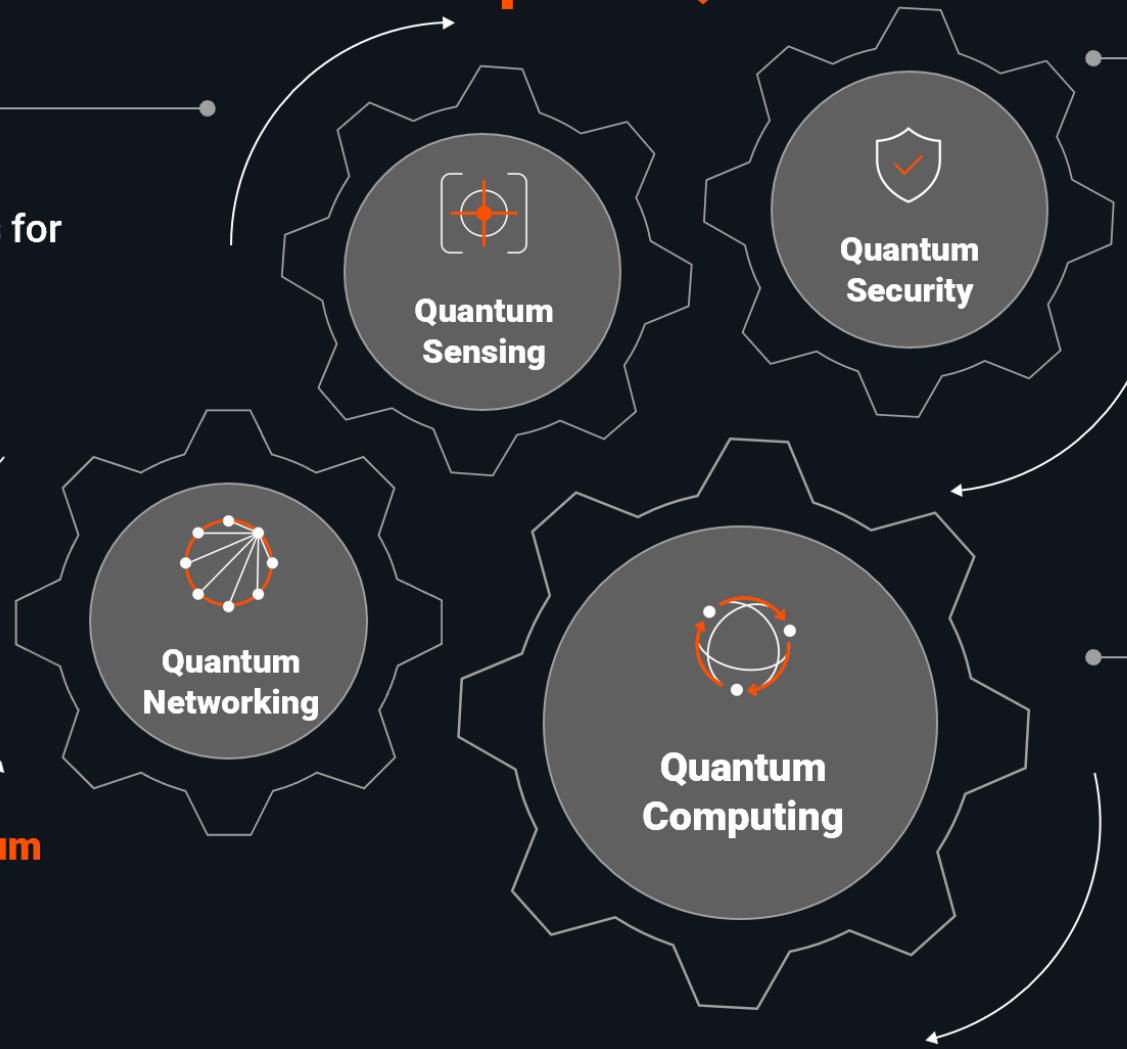
The World's Most Complete Quantum Platform



Leveraging precise measurement capabilities for **ultra high precision and accuracy**

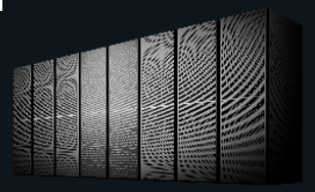


Building the **global quantum internet** for secure communications



Establishing real-world **quantum security with deployable PQC and QKD solutions**

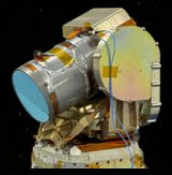
Most powerful systems for **commercial deployment**



IonQ Acquisitions

Skyloom

Enables high-speed, secure space-to-ground data transfer, reducing latency and increasing bandwidth for real-time operations

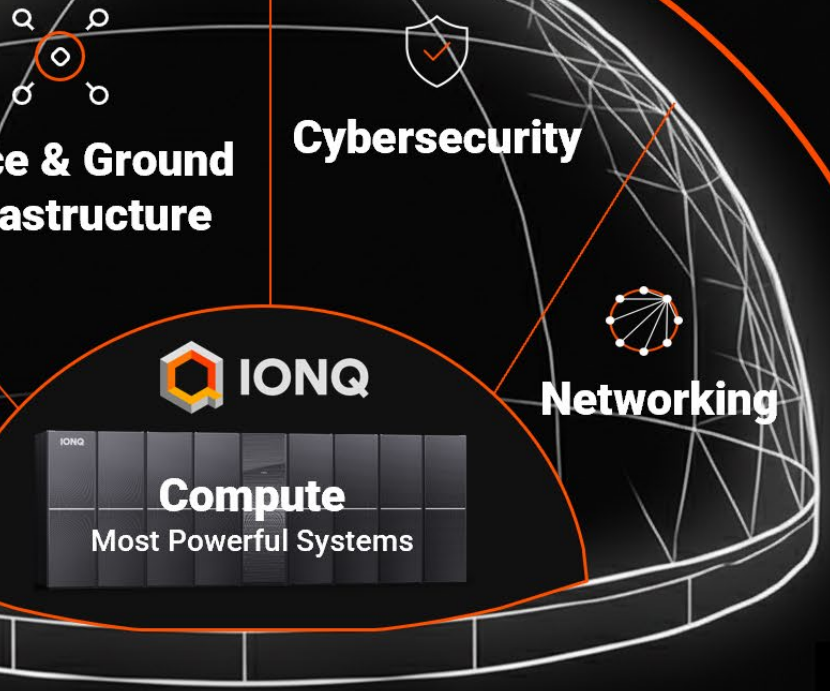


ID Quantique

QKD, PQC and quantum cybersecurity products protect all data and communications across businesses and global networks

Capella

Designs, builds, and operates advanced space systems that enable mission-ready infrastructure for space-to-ground quantum innovation and operations



Vector Atomic

Quantum sensing synchronizes systems perfectly and collects ultra-precise data for communication, data linking, and coordination

Lightsynq

Quantum Interconnects enable distributed computing and secure communication networks

IonQ Domains

A unified ecosystem leveraging physics and quantum mechanics to impact every area of technology.

Space

Quantum-enabled Space-to-Space and Space-to-Ground networks — secure PNT, intelligence, and communications from orbit

Air

Positioning, Navigation, and Timing (PNT) for GPS-denied environments

Land

Quantum-encrypted networks and the most powerful quantum computation deployable at the edge

Sea

Ultra-stable atomic clocks, GPS-free navigation, geophysical monitoring

Your Quantum Partner

Defense is driving commercialization needing assured communications, intelligence, and data sovereignty.

Contested environments demand superior positioning, navigation, and target discrimination, that legacy solutions can’t support.

Space-based processing and downlink can't keep pace with the complexity of real-time threat analysis, multi-domain fusion, and decision-making.

The Opportunity: Quantum technologies, sensors, and communications, solve these constraints across domains simultaneously.

Questions?

Thank You!

For more information, please contact:

Dr. Duncan Earl
Senior Director, Quantum Networking
duncan.earl@ionq.co

2026 SSC CYBER EXPO

PANEL

Government and Defense Contractor Cybersecurity Risks Management Policy Updates

Moderator: Ms. Brenda Taylor, SSC/S6

Panelists:

- Mr. Mathew Myhra, SSC/S6
- Mr. Shayne Douglas SSC/S6

Thank You!

For more information on CSRMC and CMMC, please contact:

Shayne Douglass
SSC/S6 Security Controls Assessor Representative, Astrion
Shayne.douglass.ctr@spaceforce.mil

Matthew Myhra
SSC/S6 A&A Branch Chief
Matthew.myhra.3@spaceforce.mil

Jacob Horne
Chief Security Evangelist, Summit 7
jacob.horne@summit7.us

Brenda Taylor
SSC/S6 Cybersecurity and Program Protection, ManTech
brenda.taylor.9.ctr@spaceforce.mil

Cody Marcus
Advisor, National Security Directorate, PNNL
cody.marcus@PNNL.gov

2026 SSC CYBER EXPO

Closing Remarks

Col Sung In
SSC/S6 Chief of Staff

Feedback Survey

Cyber Readiness at the Speed of Space