SpaceWERX Cyber Space Exchange: Shaping the Space Force's Cyber Architecture

June 30, 2026

SPACEWERX

U.S. AIR FORCE

USSF

AFRL

Next-Generation of Cybersecure and Resilient Space Vehicles

Joseph "Dan" Trujillo DR-3

AFRL Space Cyber Resiliency Program Lead

June 2026

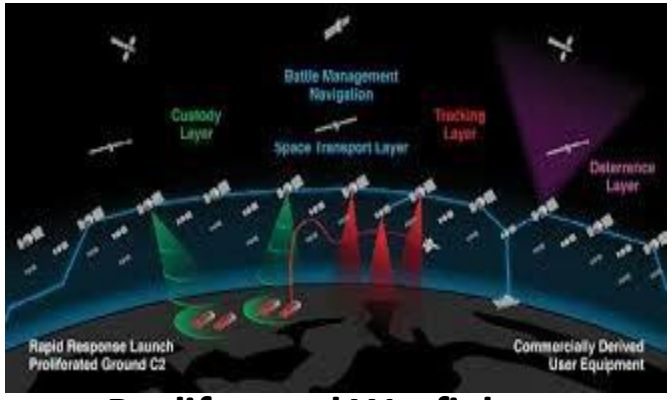
Joseph.Trujillo.4@spaceforce.mil

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

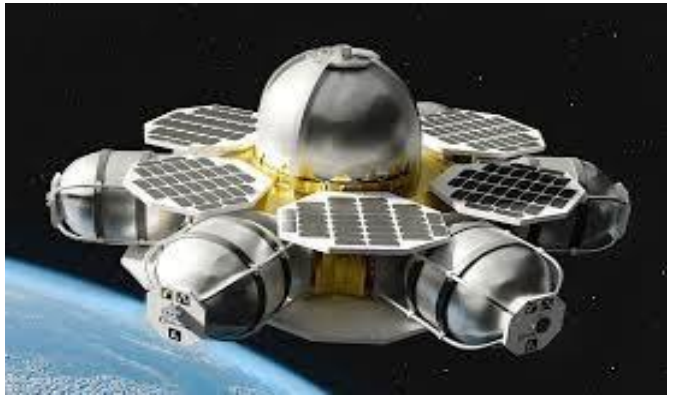


Proliferated Warfighter Space Architecture (PWSA)

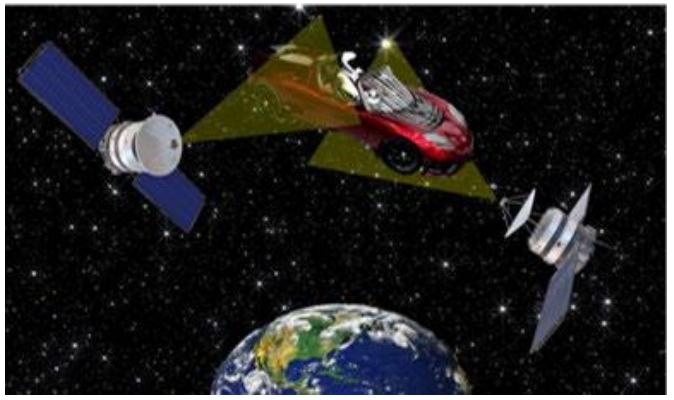
Golden Dome

Starshield & Starlink

Autonomy/Lights-out



On-Orbit Servicing/Refueling

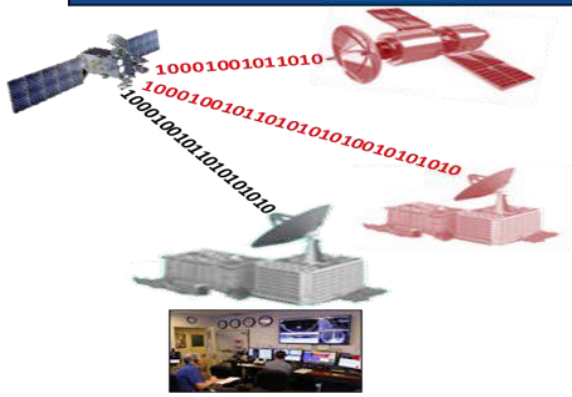


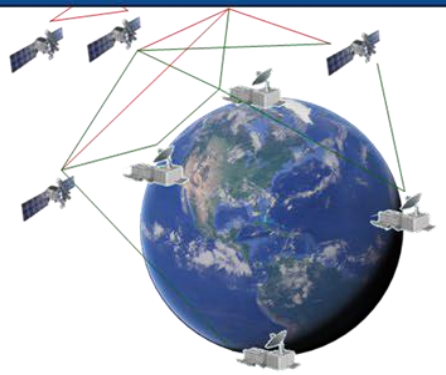
Muli-Agent/Cooperative/Inspection

Distro A

Increasing Attack Surface

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





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

+

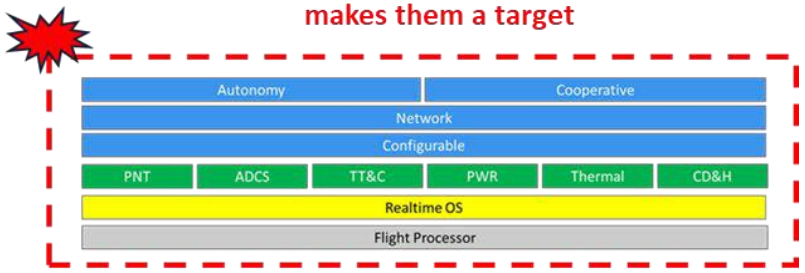
- Multi-Agent/Cooperative missions
- Autonomous systems
- Fully reconfigurable missions

- 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

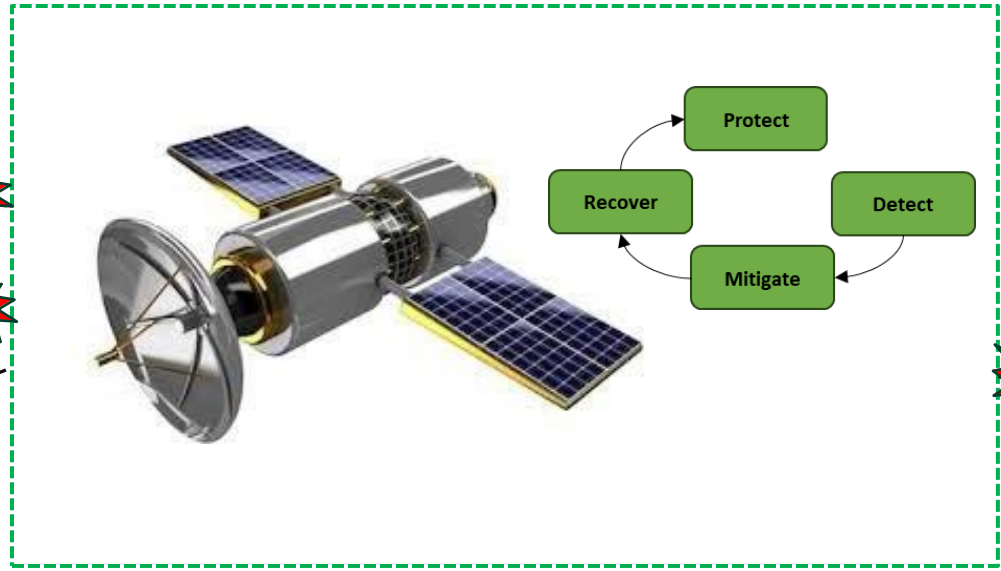
Next-Gen Cybersecure & Resilient Space Vehicles

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

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

Co-orbital

Supply Chain, Insider, compromised



Manticore/Kraken cyber Tools

Cyber Ground C2 Defensive Cyber Operations - Space

Ground-based

ENTERPRISE – Cyber Situational Awareness

Onboard capability for Space Cyber

SPACEWERX

Integrating the Space Enterprise

Col. Robert Enrico
Enterprise Capabilities, Director

Distribution Statement A. Approved for public release: distribution unlimited.

Integrate to Dominate!

SSC Org Chart

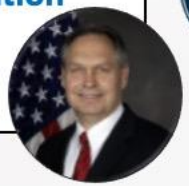
DAF PEO C3BM
Maj. Gen. Luke Cropsey

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

SASAE & SASC2I Appointments

NDAA

Administration Priorities

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

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

Integrating the Space Cyber Enterprise

Capt Adeeb Islam
Cyber Integration, Chief

Distribution Statement A. Approved for public release: distribution unlimited.

Integrate to Dominate!

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

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

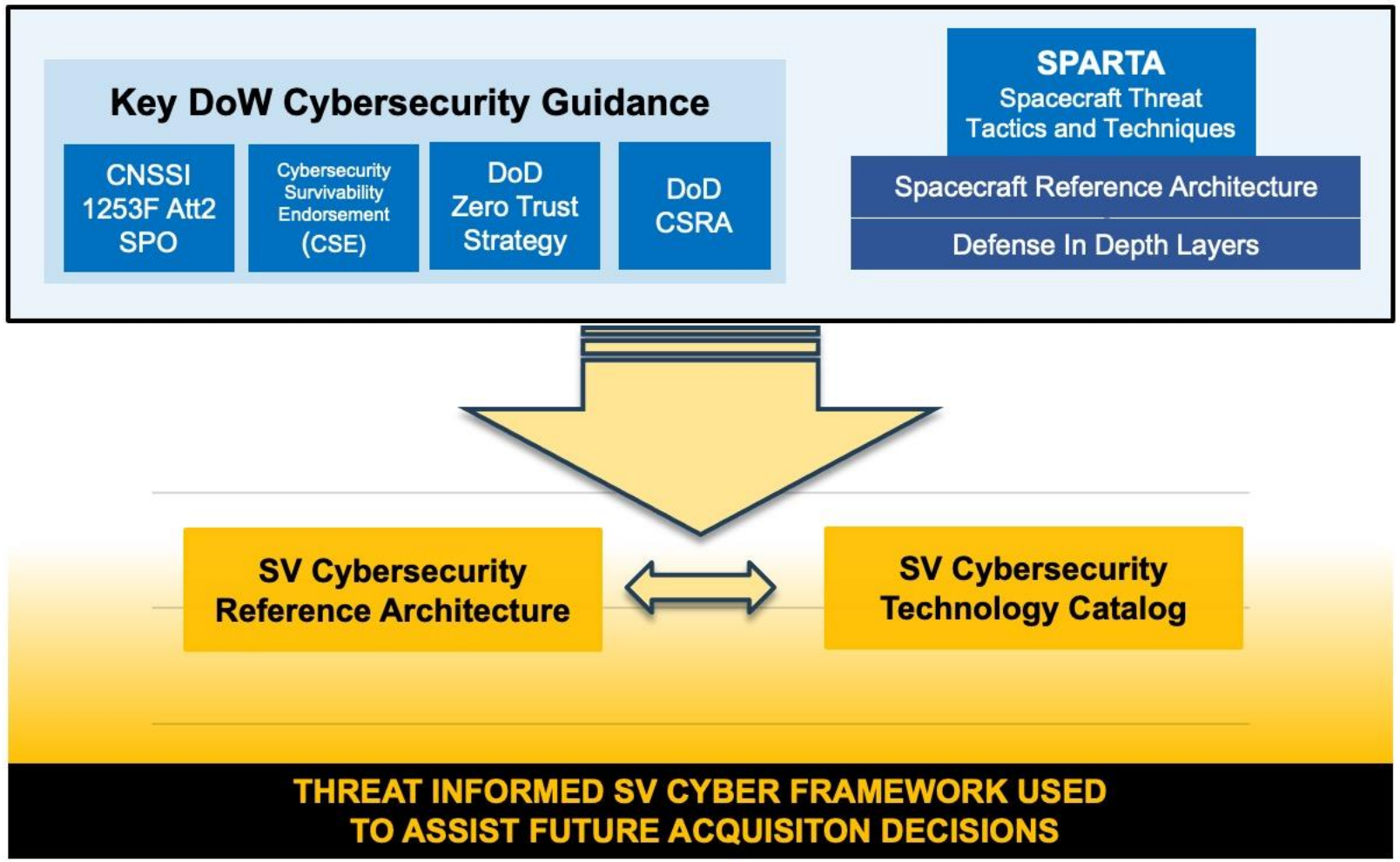
- Typical cyber protection and mitigation approaches (including zero trust) require adjustments due to unique physical access and environmental characteristics of Space Vehicles

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

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

ID-01: Identity Provisioning/ Credentials

ID-02: Mutual Authentication (Ground <> Space <> Crosslink <> Subsystem)

ID-03: Session Management & Identity-Aware Command Execution

ID-04: Authorization & Privilege Control (RBAC/ABAC/MBAC)

ID-05: Identity-Bound Data Access & Data-Centric Security

ID-06: Identity Telemetry, Monitoring & Analytics

ID-07: Intra-System Identity Validation (Internal Bus Enforcement)

ID-08: State, Mode, and Session Aware Identity Enforcement (e.g., dynamic)

ID-09: On-Orbit Credential & Key Lifecycle Management

DEVICES

DV-01: Trust Anchors (Hardware or Software)

DV-02: Secure Boot & Boot-Time Verification

DV-03: Firmware & Configuration Integrity Protection

DV-04: Runtime Integrity Monitoring & Attestation

DV-05: Device Identity & Cryptographic Binding

DV-06: Least-Privilege Hardware Access Control

DV-07: Hardware Interface Protection & Access Enforcement

DV-08: Data Protection on Devices (At Rest & In Transit)

DV-09: Device Logging, Telemetry & Trust Analytics

DV-10: Device-Level Fault Containment & Autonomous Recovery

NETWORKS

NW-01: Network Access Control & Authentication for All Links

NW-02: Network Segmentation & Micro-Segmentation

NW-03: Secure Routing, Switching & Path Validation

NW-04: Network Encryption & Cryptographic Segmentation

NW-05: Traffic Integrity, Timing & Freshness Validation

NW-06: Network Telemetry, Monitoring & Analytics

NW-07: Network Configuration Integrity & Attestation

NW-08: Dynamic Re-Keying & Cryptographic Session Management

NW-09: Network Logging & Audit

APPLICATIONS & WORKLOADS

AW-01: Workload Identity & Signature Verification

AW-02: Secure Execution Environment & Isolation Domains

AW-03: Least-Privilege Enforcement & Capability-Based Access Control

AW-04: Runtime Integrity Monitoring & Continuous Attestation

AW-05: Secure Update, Patch, & Deployment Mechanisms

AW-06: Data-Centric Protection Within Applications

AW-07: Application Behavior Monitoring, Telemetry Correlation, & Anomaly Detection

AW-08: Comprehensive Audit Logging & Onboard Policy Enforcement

DATA

DT-01: Data Classification, Labeling & Metadata Binding

DT-02: Data Encryption & Integrity Protection (At Rest, In Transit, In Use)

DT-03: Data Access Control & Least-Privilege Enforcement

DT-04: Data Provenance, Traceability & Chain-of-Custody

DT-05: Secure Data Storage, Segmentation & Compartmentalization

DT-06: Data Lifecycle Governance (Retention, Sanitization, Deletion)

DT-07: Data Audit Logging, Monitoring & Anomaly Detection

VISIBILITY & ANALYTICS

VA-01: Telemetry & Event Collection Framework

VA-02: Distributed Logging & Tamper-Evident Storage

VA-03: System-wide / Cross-domain Correlation & Analytics Engine

VA-04: Identity-bound Observability Data (telemetry, logs, etc.)

VA-05: Data Labeling, Classification, & Policy Enforcement for Telemetry

VA-06: Autonomous Detection & Onboard Response

VA-07: End-to-End Audit Fabric & Forensic Reconstruction

VA-08: Ground to Space to Crosslink Observability Integration

VA-09: Model & Rule Validation for AI/ML Analytics

AUTOMATION & ORCHESTRATION

AO-01: Policy-Driven Autonomous Decision Engine

AO-02: Cross-Domain Orchestration

AO-03: Automated Response & Containment Mechanisms

AO-04: Identity Aware Automation

AO-05: Context and Mission Aware Enforcement

AO-06: Secure Workflow & Playbook Management

AO-07: Autonomous ZPolicy Distribution & Synchronization

AO-08: Closed-Loop Detection, Decision, Enforcement Integration

AO-09: Event Provenance, Audit, and Traceability for Autonomous Actions

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

DoD CIO Reference Architecture

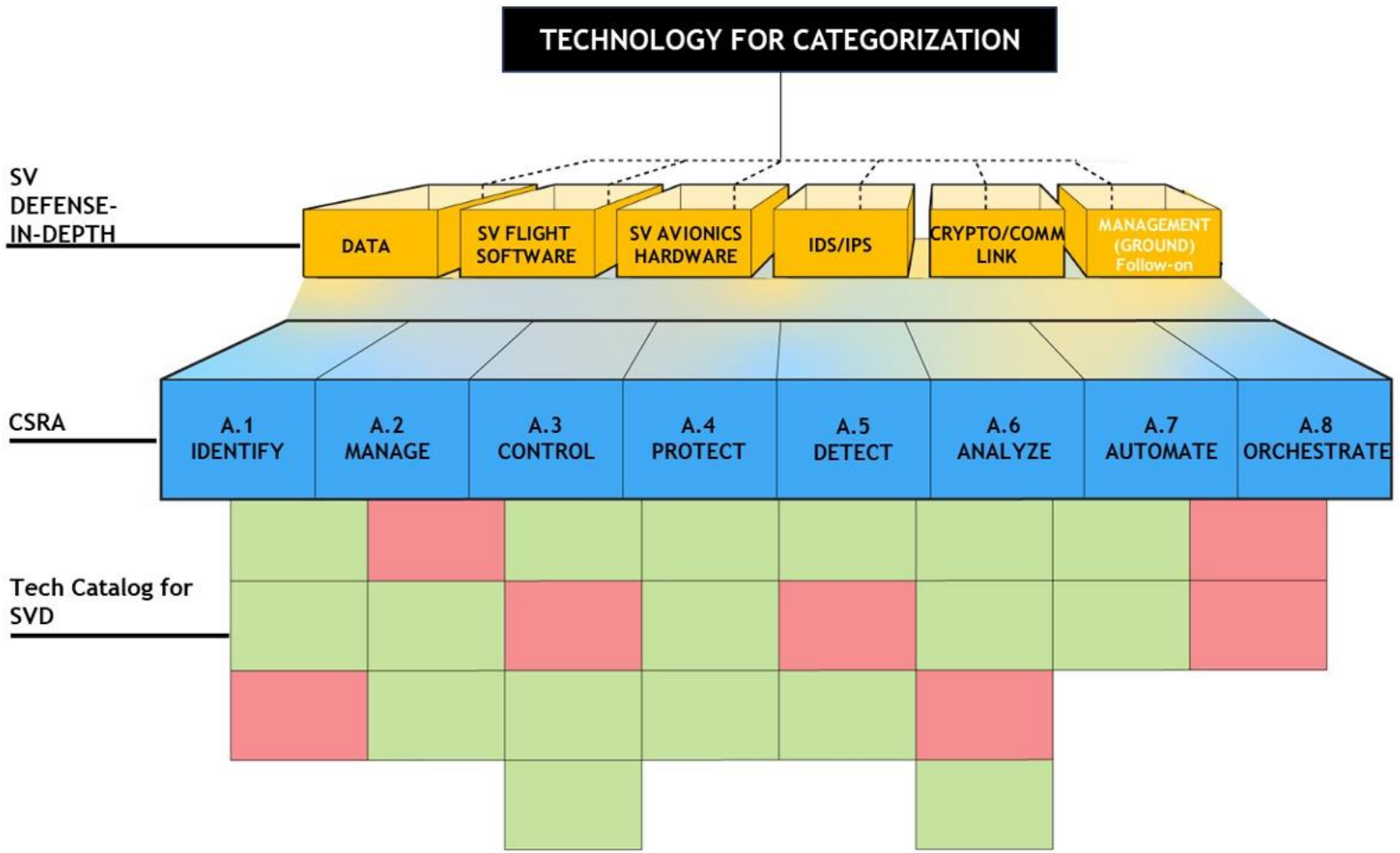
CSRA Activities and Sub-Activities

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

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)

Company Information

- Describe your company's experience in developing and integrating cybersecurity and cyber defense solutions for space systems
  - Participation in space AO cyber security events?
- Provide examples of current and previous projects demonstrating your expertise in payload integration and cybersecurity
  - Identify major primes

Technology Catalog

- Describe the specific cyber capabilities you offer that can be integrated *onboard* spacecraft within the next five years.
- How do you expect your solution to fit within the framework:
  - Defense in Depth Layer/Category
  - DoD CIO Cyber Survivability Reference Architecture Activities

Maturity, Cost & Integration

- What is the current Technology Readiness Level (TRL) of your proposed solutions?
  - Cost challenges towards TRL 9 progress
- Approach to integrating your cyber capabilities onto existing and future spacecraft architectures
  - Modularity and compatibility with various platforms
  - Impacts on spacecraft resources

Requirements Applicability

- Which portions of the following frameworks does your technology address:
  - Zero Trust
  - CNSSI 1253 App F Att 2 (Space Platform Overlay)
  - Cyber Survivability Endorsement

Next Steps

- **Engage with us today**: Let's discuss where your technologies fit for SV Cyber Defense.
- **Quad Chart Template**: Build a quad chart to be submitted; a template is provided on the following slide
- **Submit your information**: Provide comments on
  - The technology catalog framework
  - Details on your capabilities for inclusion in the Technology Catalog
- **Future Opportunities**: This catalog will be a living document, driving future requirements, informing investment decisions, and creating opportunities for collaboration

Q&A / Contact Information

Capt Adeeb Islam

adeeb.islam.1@spaceforce.mil

(310) 653 9226

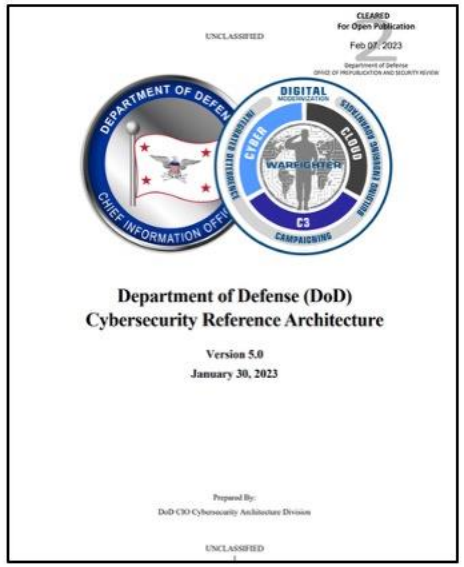
THANK YOU!

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

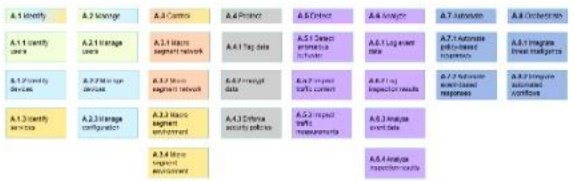
CLEARED
For Open Publication
Feb 07, 2023

Department of Defense (DoD)
Cybersecurity Reference Architecture

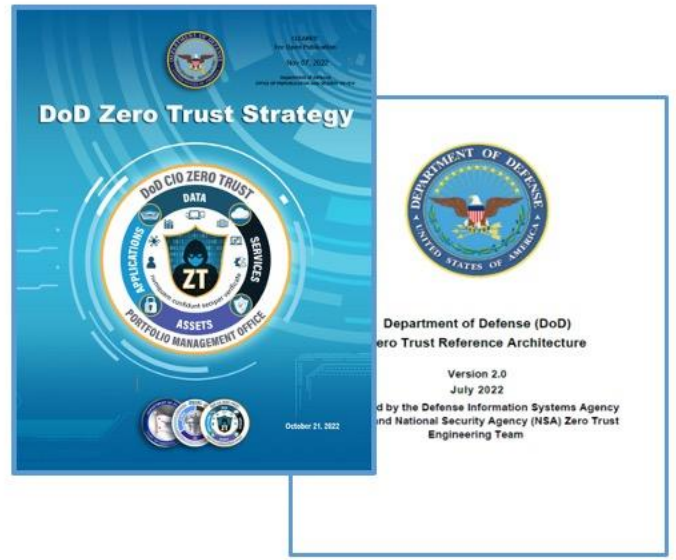
Version 5.0
January 30, 2023

Prepared By:
DoD CIO Cybersecurity Architecture Division

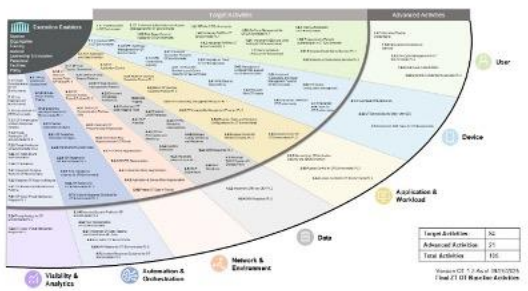
UNCLASSIFIED



DoD Zero Trust RA & Strategy



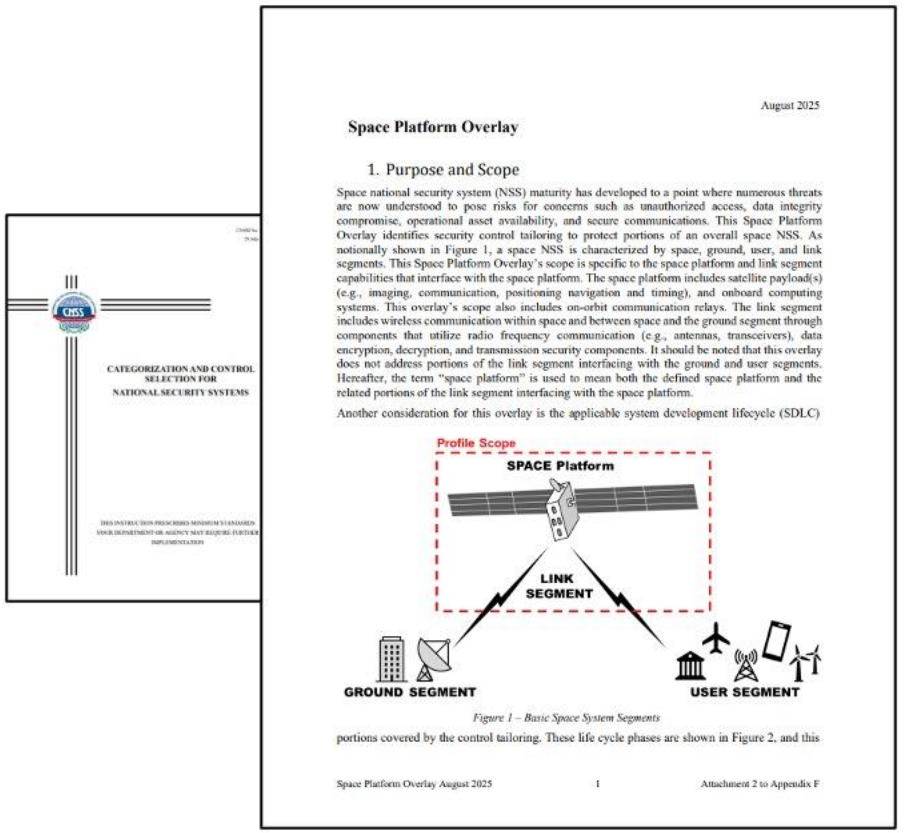
Zero Trust Fan Chart for Operational Technologies



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

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

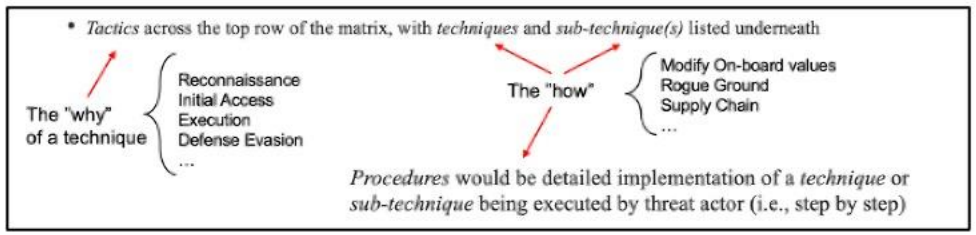
portions covered by the control tailoring. These life cycle phases are shown in Figure 2, and this

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

Build and Operate a Trusted DoWIN

Cybersecurity-Related Policies and Issuances
Developed by the DoW Deputy CIO for Cybersecurity
Last Updated: April 28, 2026
Send questions/suggestions to contact@csiac.org

Cyber Security & Information Systems Information Analysis Center

ORGANIZE

Lead and Govern

- 2025 National Security Strategy
- 2026 National Defense Strategy
- 2022 National Military Strategy (NMS)
- 2023 National Intelligence Strategy
- Cyberstrategy for America
- National Cybersecurity Strategy Implementation Plan
- National Strategy to Secure 5G
- U.S. Int'l Strategy for Cyberspace
- NIST Cybersecurity Framework
- CISA Cybersecurity Strategy Plan
- National Cyber Workforce and Education Strategy
- United States Intelligence Community Information Sharing Strategy
- 2022 DoD Zero Trust Strategy
- 2023 DoD Cyber Strategy Summary
- DoD Cyber Workforce Strategy
- Fulcrum: DoD IT Advancement Strategy
- 2023 DoD Data, Analytics, and Artificial Intelligence Adoption Strategy
- DoD CCONUS Cloud Strategy
- DoD Identity, Credential, and Access Management (ICAM) Strategy
- DoD 5G Strategy
- DoD Software Modernization Strategy
- DoD Information Security Continuous Monitoring (ISCM) Strategy
- DoD Strategy for Operations in the Information Environment
- DIB Cybersecurity Strategy

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- NIST SP 800-55 Volume 1 Measurement Guide for Information Security
- NIST SP 800-55 Volume 2 Measurement Guide for Information Security
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
- CNSS Whitepaper 20140516 National Secret Fabric Architecture Recommendations
- DoDI 5000.87 Operation of the Software Acquisition Pathway
- DoDD 5000.01 Defense Acquisition System
- DoDI 5000.02 Operation of the Adaptive Acquisition Framework
- DoDI 5200.47E Anti-Tamper (AT)
- DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
- DoDD 7045.20 Capability Portfolio Management
- DoDD O-5100.19 Critical Information Communications (CRITCOM) System
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDI 5000.82 Requirements for the Acquisition of Digital Capabilities
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- DoDD 8115.01 IT Portfolio Management
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DODAF (Version 2.02) DoD Architecture Framework
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DoDI 7000.14 Financial Management Policy and Procedures (FMPP)
- DoD Cybersecurity Reference Architecture (Version 5.0)
- CJCSI 5123.01J Charter of the JROC the JFRP
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)

Develop the Workforce

- NIST SP 800-181 R1 Workforce Framework for Cybersecurity
- CNSSI-4016 National IA Training Standard For Risk Analysts
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- DoDI 8140.02 Identification, Tracking, And Reporting of Cyberspace Workforce Requirements
- DoDD 8140.01 Cyberspace Workforce Management
- DODM 8140.03 Cyberspace Workforce Qualification and Management Program
- DoDD 5101.23E DoD Executive Agent for Advanced Cyber Training Curricula

Partner for Strength

- National Industrial Security Program Operating Manual (NISPOM) 32 CFR 117
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R3 Protecting CUI in Nonfederal Sys and Orgs (see also 800-171A, 171B)
- NIST SP 800-171 DoD Assessment Methodology (see also 800-171 R2)
- NIST SP 800-172 Enhanced Security Requirements for Protecting CUI (see also 172A)
- CNSSP-14 National Policy Governing the Release of IA Products/Services...
- CNSSP-32 Cloud Security for National Security Systems
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- Cybersecurity Maturity Model Certification (CMMC)
- DIB CS Program Security Classification Guide
- DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
- MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

- FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- NIST SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD)
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- CNSSP-520 The Use of Mobile Devices to Process Nat'l Sec. Info. Outside Secure Spaces
- NACSI-2005 Communications Security (COMSEC) End Item Modification
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm'ns
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8521.01E Department of Defense Biometrics
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8440.02 DoD Implementation of IPv6
- DoDI 8523.01 Communications Security (COMSEC)
- DoDIN S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
- CJCSI 6510.02G Cryptographic Modernization Planning

Manage Access

- FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-210 General Access Control Guidance for Cloud Systems
- NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSP-200 National Policy on Controlled Access Protection
- CNSSD-507 National Directive for ICAM Capabilities...
- CNSSD-506 National Directive to Implement PKI on Secret Networks
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSD-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.04 Access Management for DoD Information Systems
- DoDI 5200.50 Assured Access to Trusted Microelectronics
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDM 5200.48 Controlled Unclassified Information(CUI)
- DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle

Assure Information Sharing

- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDI 8170.01 Online Information Management and Electronic Messaging
- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDD 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
- CJCSI 3213.01D Joint Operations Security
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- NSTISSD-600 Communications Security Monitoring
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R5 Security & Privacy Controls for Information Systems and Orgs.
- NIST SP 800-53A R5 Assessing Security & Privacy Controls in Information Systems & Orgs.
- NIST SP 800-61, R3 Incident Response Recommendation and Considerations
- NIST SP 800-124, R2 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- NIST SP 800-163, R1 Vetting the Security of Mobile Applications
- NIST SP 800-218 Secure Software Development Framework (SSDF)
- NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
- CNSSD-504 Protecting National Security Systems from Insider Threat
- CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
- CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDM 8530.01 Cybersecurity Activities Support Procedures
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoDI 8530.03 Cyber Incident Response
- DoDI 8531.01, DoD Vulnerability Management
- DoDI 5205.16 DoD Insider Threat Program
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- DTM-24-001 DoD Cybersecurity Activities Performed for Cloud Service Offerings
- CJCSM 6510.02 IA Vulnerability Mgt Program
- CJCSM 6510.01B Cyber Incident Handling Program
- Joint Publication 6-0 Joint Communications System

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking* on the box directs users to the most authoritative publicly accessible source.
- *Policies in Italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The listed sites are not controlled by the developers of this chart. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site, based on site architecture.

*Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.

For the latest version of this chart or email alerts to updates go to https://csiac.dtic.mil/resources/the-dod-cybersecurity-policy-chart/

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

PREPARE

Develop and Maintain Trust

- CNSSP-12 CS Policy for Space Systems Used to Support Nat'l Sec. Missions
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- CNSS 1200 National CS Inst. for Space Systems Used to Support Nat'l Sec. Missions
- NIST SP 800-160, Vol.1 Rev.1, Engineering of Trustworthy Secure Systems
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

- NIST SP 800-207 Zero Trust Architecture
- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-39 Managing Information Security Risk
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 800-161 Rev 1 Cybersecurity Supply Chain Risk Management Practices
- NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
- NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
- NIST SP 800-221 Enterprise Impact of Information and Communications Technology Risk
- NIST SP 1800-35 Implementing a Zero Trust Architecture: High Level Document
- CNSSD-505 Supply Chain Risk Management
- CNSSI-1015 Enterprise Audit Management (EAM) for National Security Systems (NSS)
- DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JCC2)
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems / Networks
- DoDI 8560.01 COMSEC Monitoring
- DoDI 8500.01 Cybersecurity
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- DTM 25-003, Ch 1 Implementing the DoD Zero Trust Strategy

Sustain Missions

- NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-82, R3 Guide to Operational Technology (OT) Security
- CNSSP-18 National Policy on Classified Information Spillage
- CNSSP-22, IA Risk Management Policy for National Security Systems
- CNSSP-300 National Policy on Control of Compromising Emanations
- CNSSI-1001 National Instruction on Classified Information Spillage
- CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-7000 TEMPEST Countermeasures for Facilities
- NSTISSI-7001 NONSTOP Countermeasures
- Acquisition Guidebooks
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
- DoDD 5144.02 DoD Chief Information Officer
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 8410.03 Support to DoD Information Network Operations
- DoDD 3020.26 DoD Continuity Policy
- DoDM 5000.103 Cyber developmental Test and Evaluation
- DoDD 5000.83 Technology & Program Protection to Maintain Technological Advantage
- ICD 503 IT Systems Security Risk Management and C&A
- NSA IA Directorate (IAD) Management Directive MD-130 Cryptographic Key Protection

Legend

DOD CIO · CNSS/NSTISS · DISA · DAI · JCS · MAP · NIST · NSA · OSD · CYBERCOM · USD(A&S) · USD(C) · USD(I&S) · USD(P&R) · Other Entities · Updated Policy · Updated Hyperlink · CAC Req'd

AUTHORITIES

- Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14, US Code Cooperation With Other Agencies (Ch. 7)
- Title 32, US Code National Guard (§102)
- Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44, US Code Federal Information Security Mod. Act, (Chapter 35)
- Title 50, US Code War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Information Security Modernization Act (2014)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 (as amended) Critical Infrastructure Protection in the Info Age
- EO 13587 Structural Reforms To Improve Classified Nets
- EO 13636: Improving Critical Infrastructure Cybersecurity
- EO 13691 Promoting Private Sector Cybersecurity Information Sharing
- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- EO 13873: Securing the Information and Communications Technology and Services Supply Chain
- EO 14028: Improving the Nation's Cybersecurity
- EO 14117: Preventing Access to Americans' Sensitive / US Government Data by Countries of Concern
- EO 14306 Sustaining Select Efforts To Strengthen the Nation's Cybersecurity
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- PPD 21: Critical Infrastructure Security and Resilience
- PPD 28, Signals Intelligence Activities
- PPD 41: United States Cyber Incident Coordination
- A-130, Management of Fed Info Resources
- FAR Federal Acquisition Regulation
- Joint Special Access Program (SAP) Implementation Guide (JSIG)
- NIST Special Publication 800-Series
- NIST SP 800-63-4 series Digital Identity Guidelines
- NIST SP 800-88, R2,Guidelines for Media Sanitization
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM)
- NIST SP 800-209 Security Guidelines for Storage Infrastructure
- NISTIR 7298, R3, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSI-4009 Cmte on National Security Systems Glossary
- DoD Information Technology Environment Strategic Plan
- RMF Knowledge Service

OPERATIONAL/SUBORDINATE POLICY

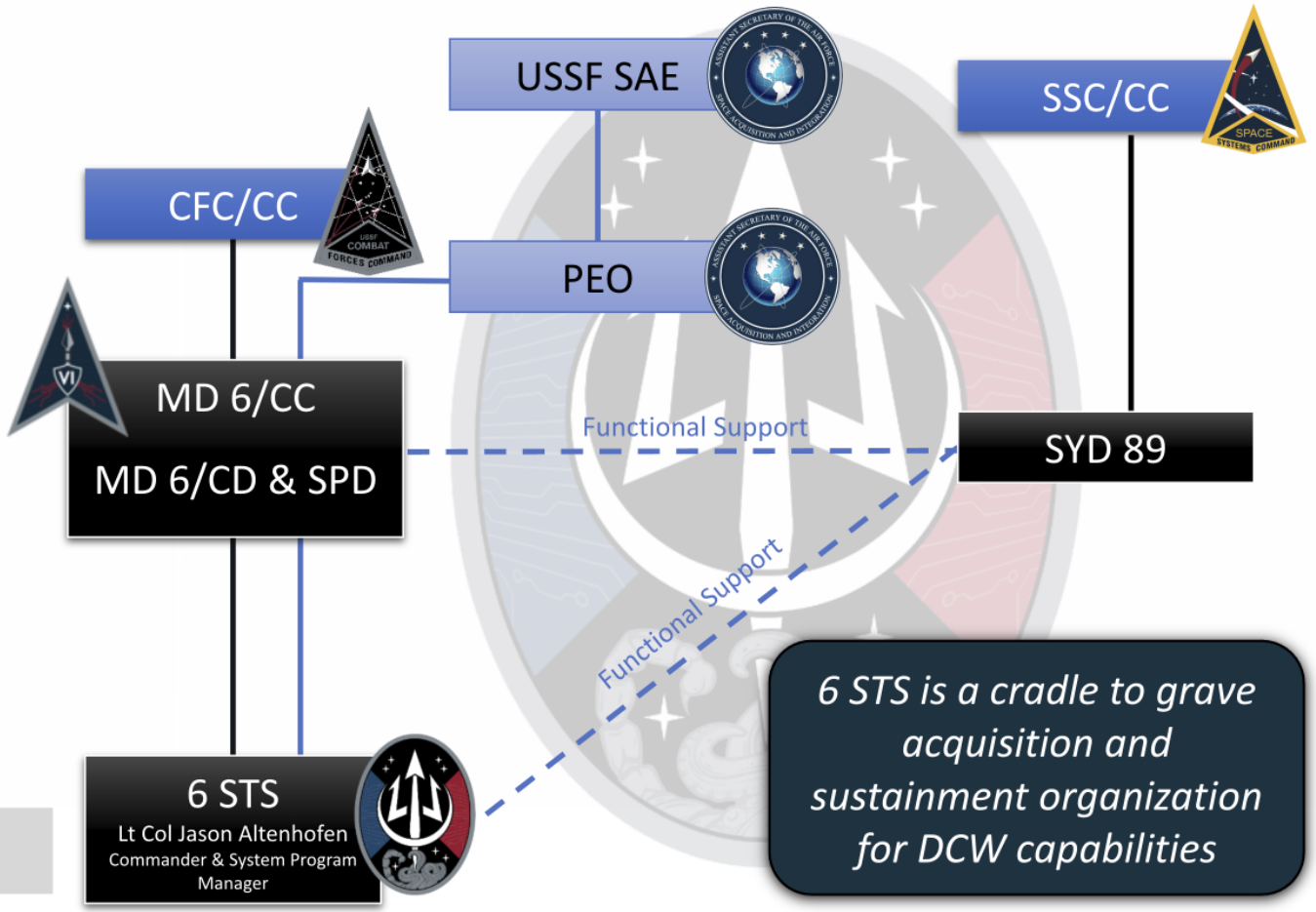
- CYBERCOM Orders
- DCDC Orders
- DoD Security Classification Guides
- NSA CS Advisories and Guidance
- Component-level Policy (Directives, Instructions, Publications, Memoranda)
- STIGs, SRGs, and TCGs

SPACEWERX

6 STS
SSIO COLLIDER EVENT
CAPT HARELD
KIM COLGAN

Integrated Mission Delta Posture

- **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

Questions

SPACEWERX

SpaceWERX Cyber Space Exchange Webinar Survey