

Hybrid Satellite Networks (HSN) Cybersecurity Framework Profile DRAFT Annotated Outline (AO)

National Cybersecurity Center of Excellence

Joseph Vanderpoorten NH-04 / USSF

James McCarthy / NCCOE

Dan Mamula / MITRE

Joe Brule / MITRE

08/11/2022



This webinar is being recorded

NIST Welcome and Introduction

James McCarthy, NCCOE

08/11/2022

Agenda

- NIST welcome and overview – Jim McCarthy NIST
- SSC keynote – Joseph Vanderpoorten USSF
- HSN cybersecurity background – Dan Mamula MITRE
- AO outline – Joseph Brule MITRE
 - Overview
 - Comment review
 - HSN COI
- Discussion

Overview of NIST Cybersecurity Profiles for the Space Sector

- Executive Order (EO) 13905 (02/12/2020); *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.*
 - US Dept. of Commerce / NIST – tasked with creation of “profiles” for Positioning Navigation and Timing (PNT) EO
 - Cybersecurity Profile for the Responsible Use of Positioning, Navigation and Timing (PNT) Services delivered February 2021 – Focused on PNT User Segment
 - NISTIR 8323 Revision 1 – draft currently out for public comment
 - No material changes to original Profile
 - Added 5 new CSF Subcategories
 - Added 2 appendices
 - Update informative references
 - Comment period closes 08/12/2022

Overview of NIST Cybersecurity Profiles for the Space Sector (continued);

- Profile activity since;
 - **Ground Segment (Draft NISTIR 8401)**
 - Final document expected Q4 FY2022
 - **Space Vehicle (Draft NISTIR 8270)**
 - Comment adjudication underway and final document TBD
 - **Hybrid Satellite Networks (HSN) Annotated Outline (AO)**
 - AO establishes content of draft HSN Cybersecurity Profile
 - Profile work to begin Q1 FY 2023

NIST Cybersecurity Framework



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

Content of a Sector Level Profile

Guidance on how to apply the subcategory to sector

Function

Category

Subcategory

Subcategory ID

CSF language

Identify: Asset Management Category		
Subcategory	Applicability to the ground segment	References
ID.AM-1: Physical devices and systems within the organization are inventoried.	Document and maintain an inventory of the components to include cloud-based resources that reflect the current system. Consider incorporating a configuration management tool that documents the physical location of all physical components and verify with physical inspections. During physical inspections, identify equipment and its physical interfaces.	NIST SP 800-53 Rev. 5 CM-8, CM-9 PM-5 NIST SP 800-160 Rev. 1 2.3
ID.AM-2: Software platforms and applications within the organization are inventoried.	Document and maintain an inventory of software components to include virtual machine images, such as license information, version numbers for applications, software and operating systems. System software inventory is reviewed and updated as defined by the organization.	NIST SP 800-53 Rev. 5 CM-8, PM-5 NIST SP 800-204C

Specific references to provide insight on applying controls to achieve the desired outcomes.

Keynote Address

Joe Vanderpoorten, Space Systems Command

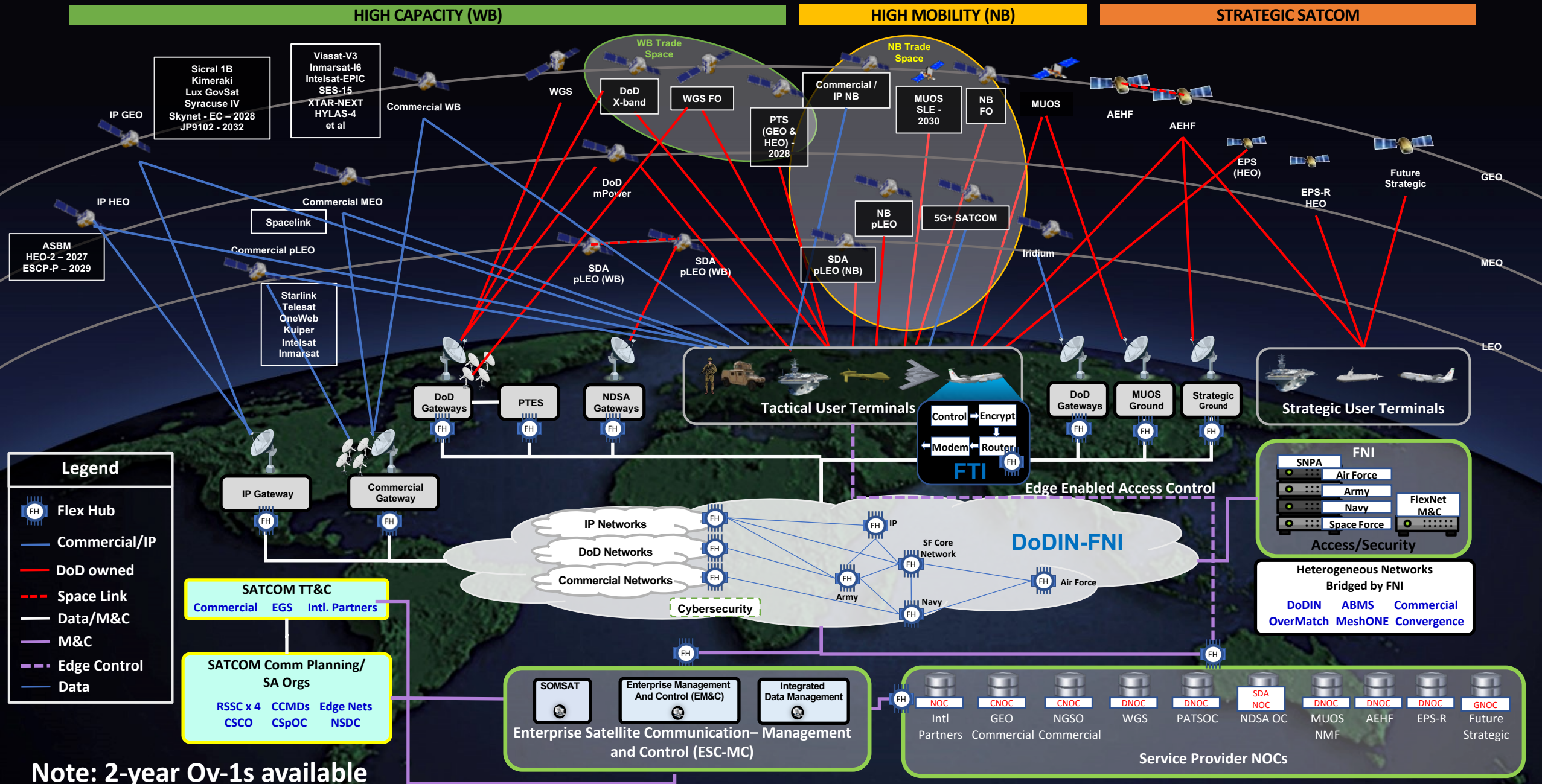
08/11/2022



Joe Vanderpoorten, NH-04
SATCOM Technical Director
PEO for SATCOM and Navigation
Space Systems Command
US Space Force

Joseph.Vanderpoorten@spaceforce.mil

SATCOM Hybrid Architecture (2032) OV-1



Characteristics

Integrated operations (goal)

Collective Cyber Defense

Heterogenous Product Sourcing

Multiple Point Control

Numerous attack vectors



Cyber Application to Satellite Communications

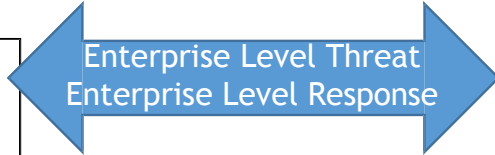
US, UK and EU blame Russia for 'unacceptable' Viasat cyberattack



Ukrainian KaSat Attack

Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds

The New York Times



Speaks to End to End SATCOM Enterprise (against next generation threats?)

United States Space Force Vision for Satellite Communications (SATCOM)

SATCOM Vision

23 January 2020

Distribution A: Approved for public release; distribution unlimited

Technology Roadmap: Airborne Intelligence, Surveillance, and Reconnaissance (AISR) Platform Data Transport

December 2021

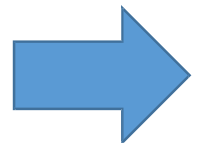
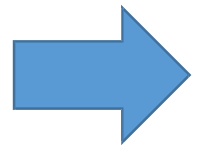
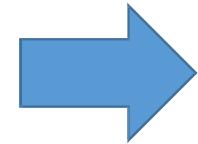


Sophisticated Enterprise Attack - Need AISR Enterprise Response?



Generic Threat Visualization
Actuals →

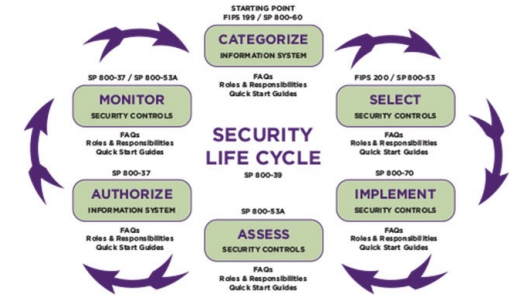
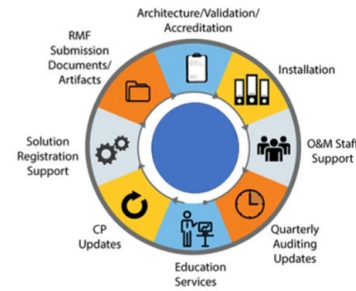
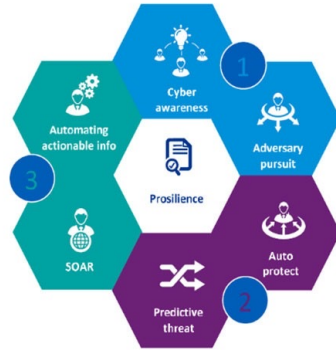
Primary Space Cyber Threats



Threat	Description	Insertion Points	Mitigations	Metadata/Metric
DOS/DDOS and associated attacks	Denial of Service Attacks or Distributed Denial of Service (DDoS) attacks are much concern to the SATCOM industry. Mostly effecting terrestrial nodes.	Boundary equipment	NextGen Firewalls utilizing Advanced Threat Detection or Prevention services & Boolean based Intrusion Detection or Prevention System (IDS)/(IPS) on the network boarder.	Metadata polled form boundary equipment into an SIEM database and forwarded to USSF CSOC and USCYBERCOM.
PAS	Polymorphic Attach Surfaces are becoming more prominent cyber threats.	Localized machines on internal network	Signature based detection & prevention systems. Pulling from multiple threat cloud sources.	Metadata polled form equipment into an SIEM database and forwarded to USSF CSOC and USCYBERCOM.
0-Day	Zero Day Attacks are familiar attack vectors or surfaces exploited usually months prior.	Internal, Boundary, and External network nodes	Signature based detection & prevention systems. Boolean Machine learning technologies.	Metadata polled form equipment into an SIEM database and forwarded to USSF CSOC and USCYBERCOM.
MitM	Man-in-the-Middle attacks threaten national security when Mission Downlink (MDL) traffic is attacked and Telemetry, Tracking & Control (TT&C) for space operations.	Internet / Boundary equipment exploit	Encryptions, solutions such as Commercial Solutions for Classified (CSfC), WireGuard, and similar solutions for obfuscation.	Metadata polled form boundary equipment into an SIEM database and forwarded to USSF CSOC and USCYBERCOM.
SSCM Exploits	Secure Supply Chain Management is a threat for the technologies coming out of China, it is known that technologies are riddled with microchips made to sniff traffic and create backdoor and exploits.	Internal, Boundary, and External network nodes	Vetted Approved Products List (APL)	Secure supply chain and metadata polleA1:E6d form boundary equipment into an SIEM database and forwarded to USSF CSOC and USCYBERCOM.

*Note: The list above is not exhaustive. Other methods of mitigation are to implement a Zero Trust Architecture (ZTA) and the utilization of new cryptography like quantum encryption.

Alignment to USSF



Feature	Description	Benefit	ISCM
Cyber Awareness	Automatically merges standard network scans with device configurations	Real-time Situational Awareness	Define / Establish
Adversary Pursuit	Autonomous and manned defensive tools and operation	Real-time operation threat hunting	Implement
Auto Protect	Guardrail "Change Direction" "execution", code deployment	Stop malicious attacks before they execute	Implement
Predictive threat	Highly-intelligent, machine-learning that auto-detects threats	Prepare and defend against future threats	Analyze / Report
SOAR	Security Orchestration, Automation and Response, quickly discern the criticality and legitimacy of an alert	User & Entity Behavioral Analytic tools such as Bay Dynamics; Advanced Threat Detections Tools, and; Sandbox	Respond
Automating Actionable info	Sort unnecessary logs, filters and prioritizes data.	Automated Security Information and Event Management (SIEM) and reporting	Review / Update

1. COMSATCOM IA-Pre Framework
Evolve to new **NIST Cyber Security Framework**
2. Position “Red team” to outpace adversary
3. Posit for full path diversity – over whelm attack vector prospects through “day of” resets

HSN Background

Dan Mamula / MITRE

08/11/2022

Background and Purpose: HSN Cybersecurity

NIST



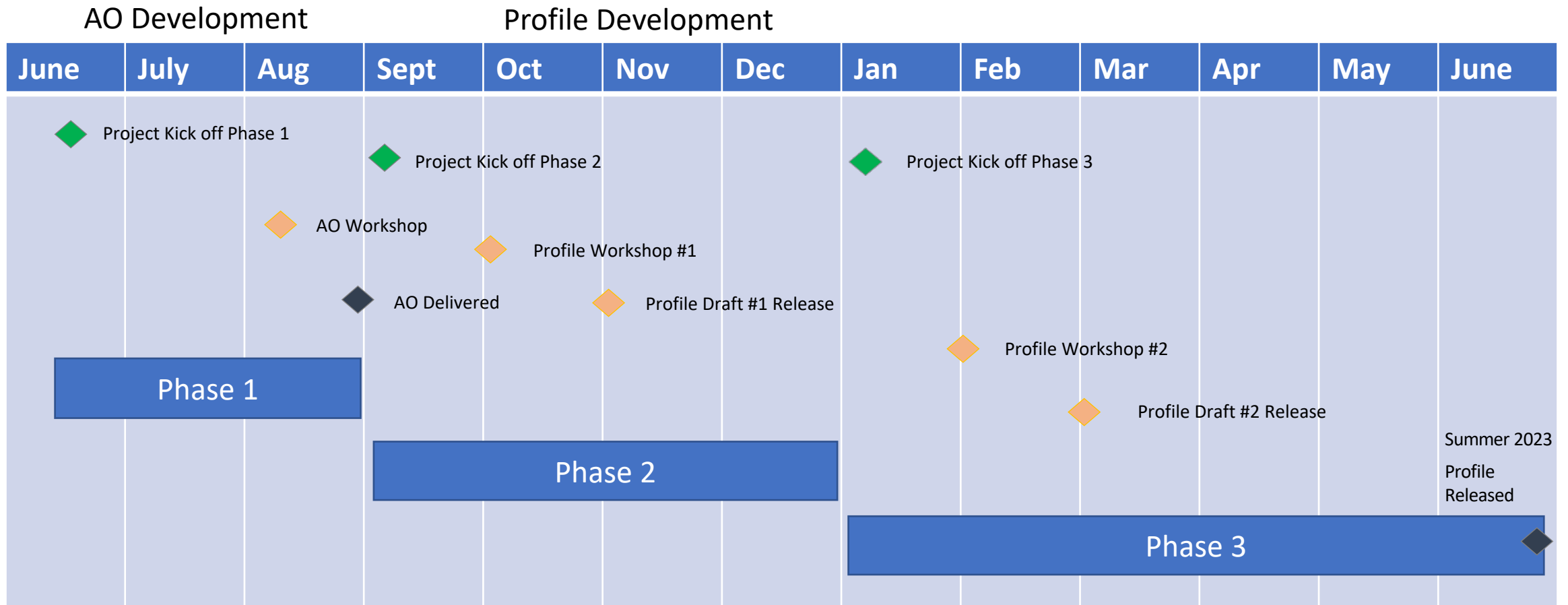
- What is HSN cybersecurity?
 - A space-based capability that is provided by the private, commercial sector to the government
 - A hosted payload is one easy example, there are many more
- What is an Annotated Outline (AO)?
 - Used to create the structure for Profile development
- Purpose
 - Develop a Profile on the topic of cybersecurity of Hybrid Space Systems. The profile will be published in the form of an NIST interagency Report (NISTIR) that will be made available to the public. This will help the Space Force to develop a common language and best practices with industry on cybersecurity of future hybrid satellite networks.

HSN CSF Profile Phases

- The profile will be developed in three phases
 - Phase 1
 - Establish a community of interest
 - Publish and Collect responses to an RFI on the topic
 - Publish an annotated outline of the profile and get feedback from industry
 - Phase 2
 - Analyze comments from phase 1
 - Hold community workshop on Cyber Security for space systems
 - Publish the first draft of the profile
 - Phase 3
 - Analyze feedback from first draft
 - Hold workshop 2
 - Final profile (NISTIR) is released

HSN CSF Profile Preliminary Schedule

◆ Delivery
◆ Milestone



HSN Annotated Outline

Overview and Comment Review

Joe Brule/ MITRE

08/11/2022

Annotated Outline

- Section 1
 - Provides Background, Scope and Target Audience
- Section 2
 - Purpose, Intended Use and Benefits of the CSF
- Section 3
 - Review of Risk Management
 - Overview of Capabilities
 - The Profile
 - Brief Description of the Subset of the CSF Applicable to HSN
 - Informative References to Guide the Reader

Content of a Sector Level Profile



Guidance on how to apply the subcategory to sector

Function

Category

Subcategory

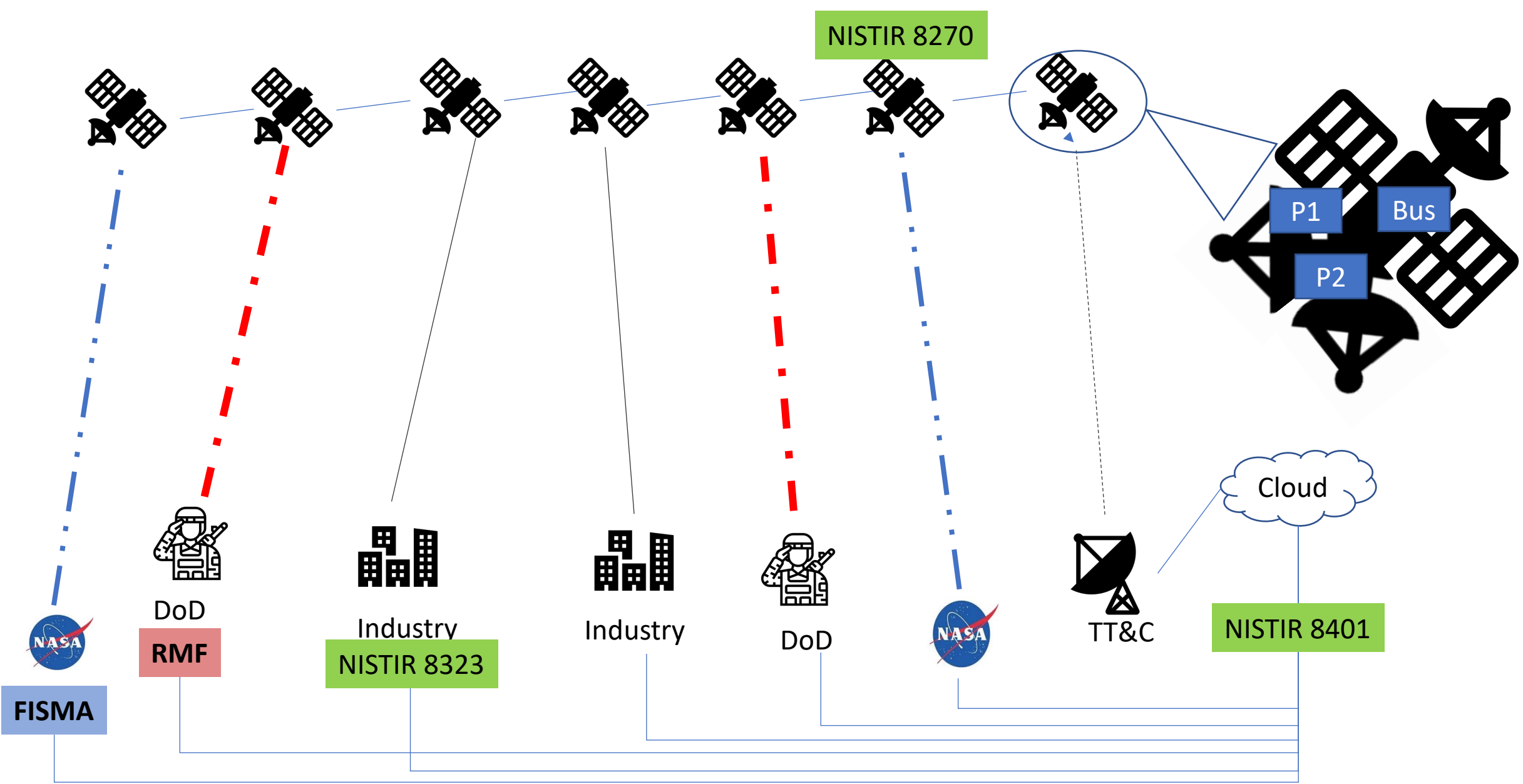
Subcategory ID

CSF language

Identify:		
Asset Management Category		
Subcategory	Applicability to the ground segment	References
ID.AM-1: Physical devices and systems within the organization are inventoried.	Document and maintain an inventory of the components to include cloud-based resources that reflect the current system. Consider incorporating a configuration management tool that documents the physical location of all physical components and verify with physical inspections. During physical inspections, identify equipment and its physical interfaces.	NIST SP 800-53 Rev. 5 CM-8, CM-9 PM-5 NIST SP 800-160 Rev. 1 2.3
ID.AM-2: Software platforms and applications within the organization are inventoried.	Document and maintain an inventory of software components to include virtual machine images, such as license information, version numbers for applications, software and operating systems. System software inventory is reviewed and updated as defined by the organization.	NIST SP 800-53 Rev. 5 CM-8, PM-5 NIST SP 800-204C

Specific references to provide insight on applying controls to achieve the desired outcomes.

- Six Sets of Reviews
 - Satellite Operators, Satellite Vendors, Security Consultants, and University
- Comments
 - Emphasize HSN cyber-security posture (rather the organization)
 - HSN Definition: Need Additional Detail
 - Include Cybersecurity Architects in the Audience
 - Section 3.3 is Incomplete and Doesn't Align with CSF functions
- Multiple comments suggested defining/scoping of the Profile
 - Need to refine scope
 - Space vehicle itself needs more attention
 - Securing a Government payload on a commercial host
 - Space Domain needs to be complimentary with other efforts
 - NISTIRs 8323, 8270, 8401



HSN Community of Interest

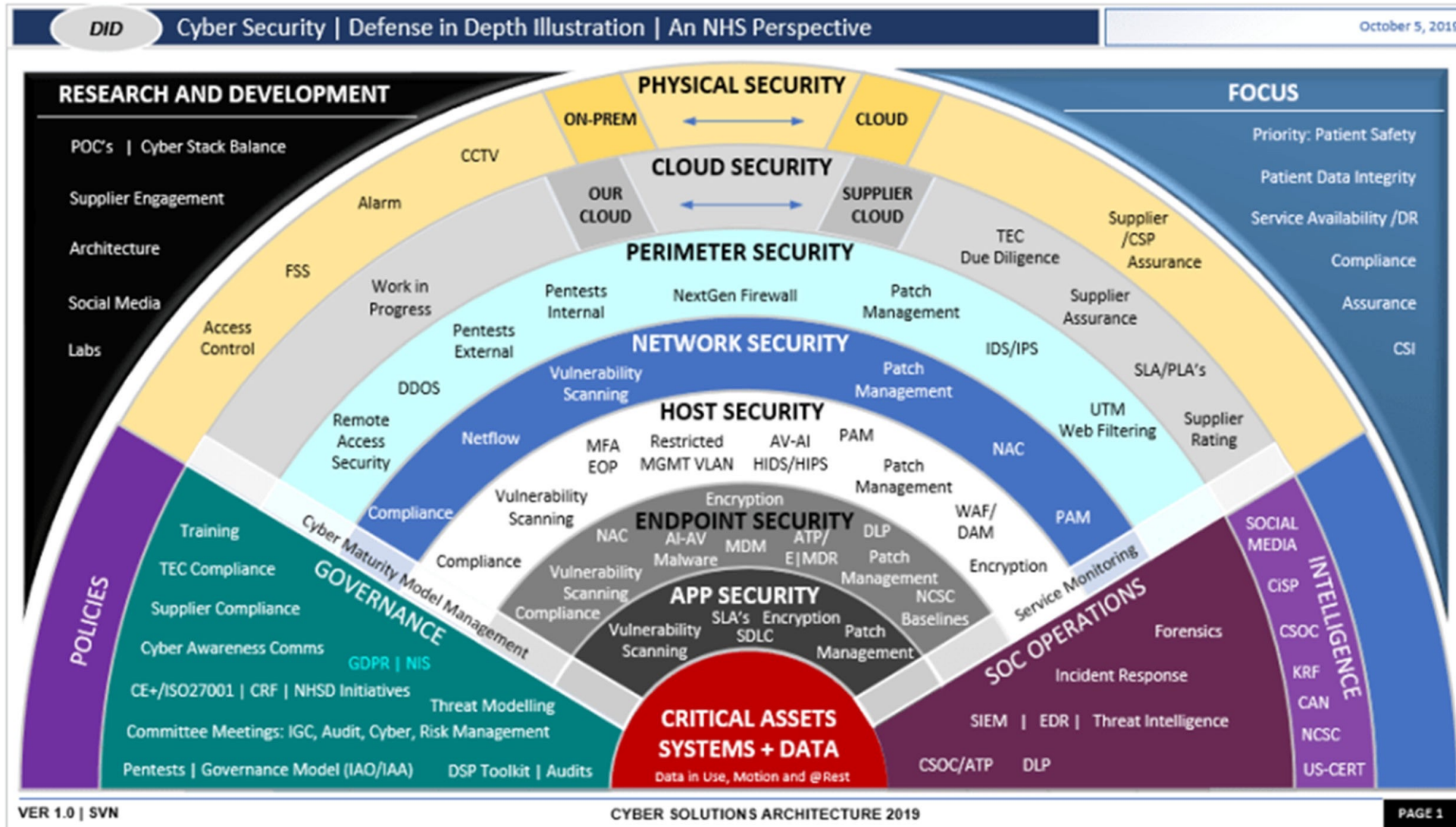


- Community Driven Effort to Produce a Draft
- Tempo
 - Biweekly Web-conferences
 - Comment submission/ resolution between meetings
 - Optional Deep Dives
- Members
 - Satellite Operators
 - Satellite Vendors
 - Government
 - Academia
 - Consultants
- Join by Contacting [HSN COI](#) (Currently 35 Members)
 - Feel Free to Forward to Other Stakeholders

Backups

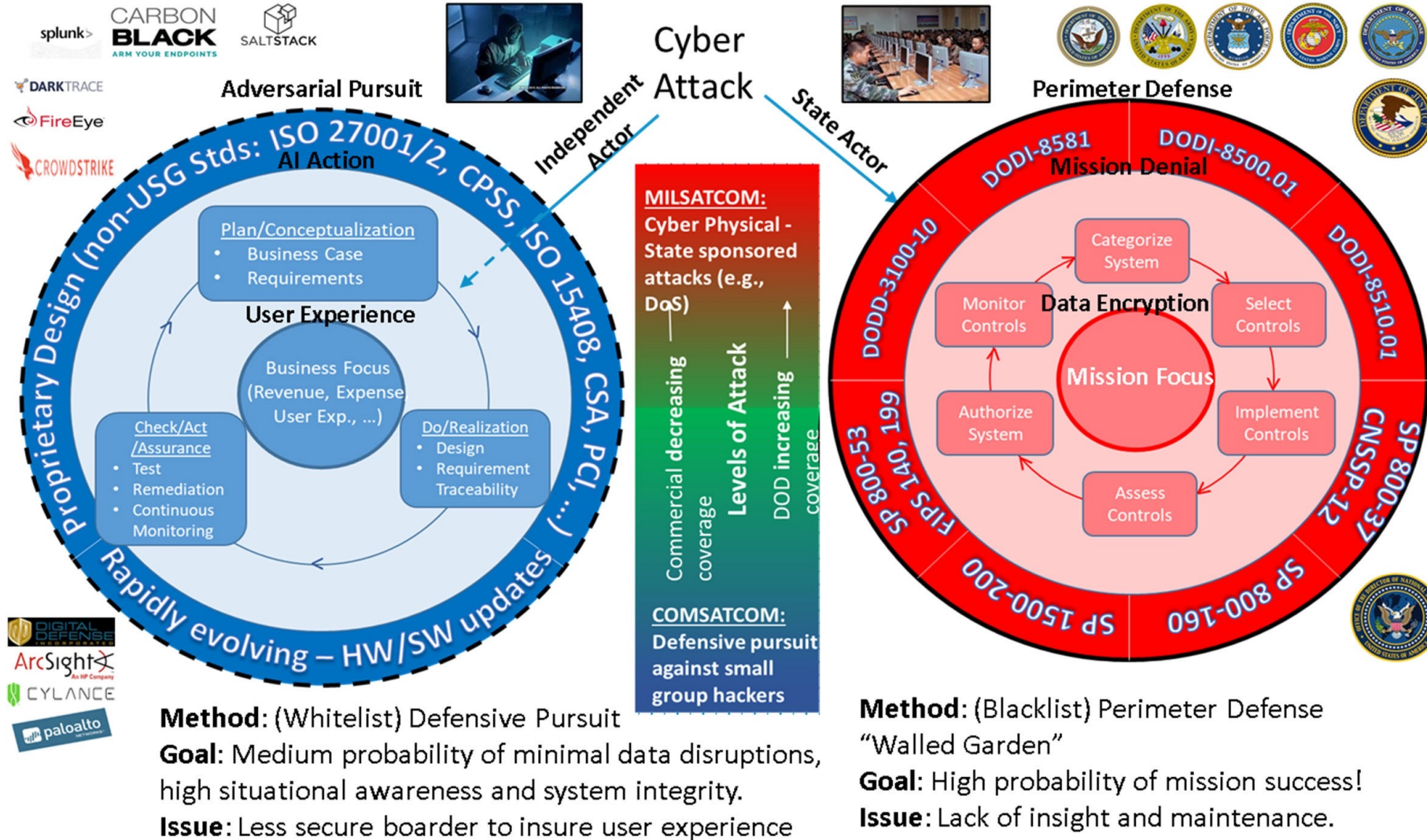


Defense-in-Depth



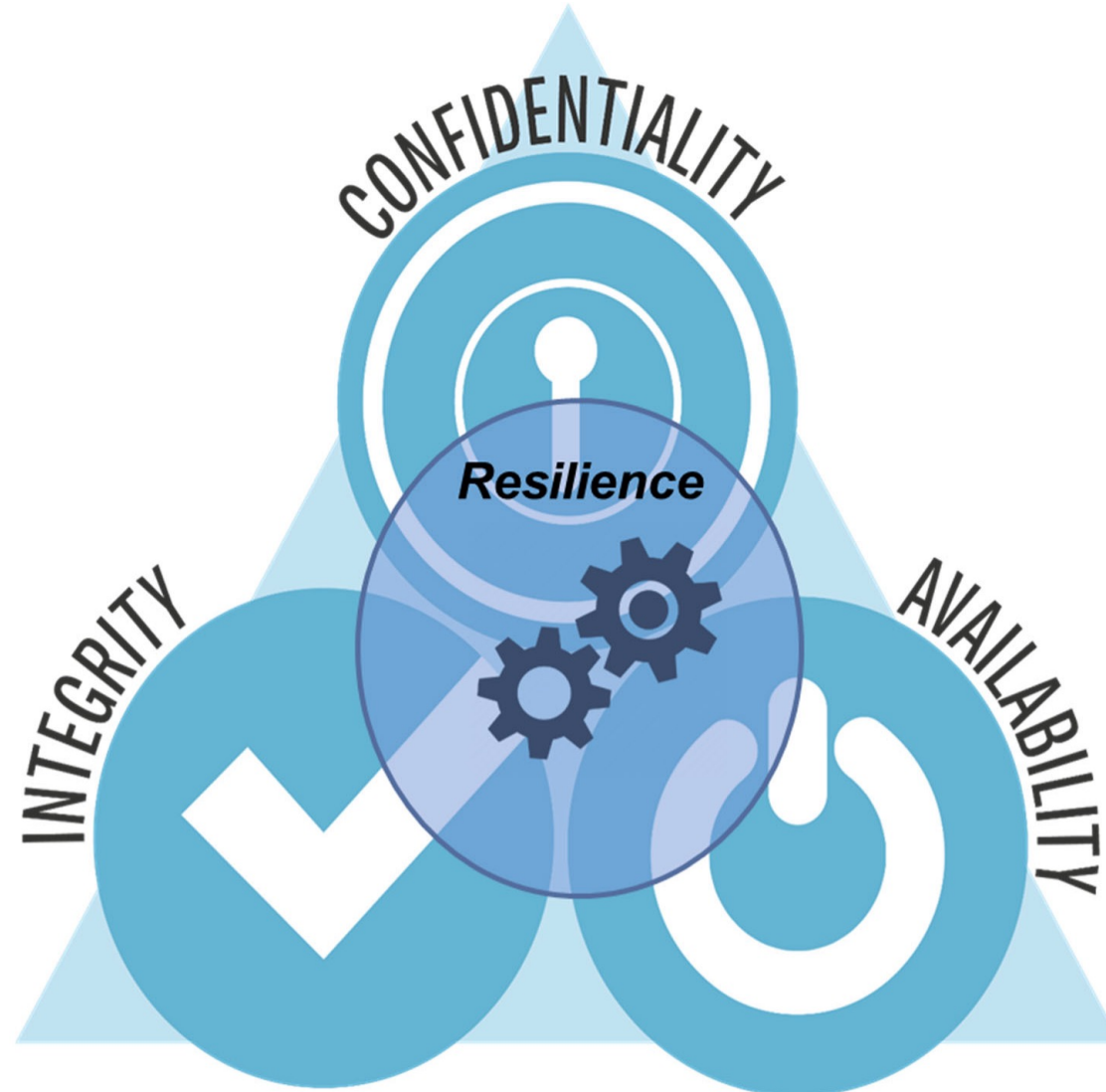


COMSATCOM v. MILSATCOM





Overlap of CIA = Resilience





Navigating and Adhering to Complex Policies



Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: June 24, 2022
Send questions/suggestions to contact@csiac.org

ORGANIZE
Lead and Govern

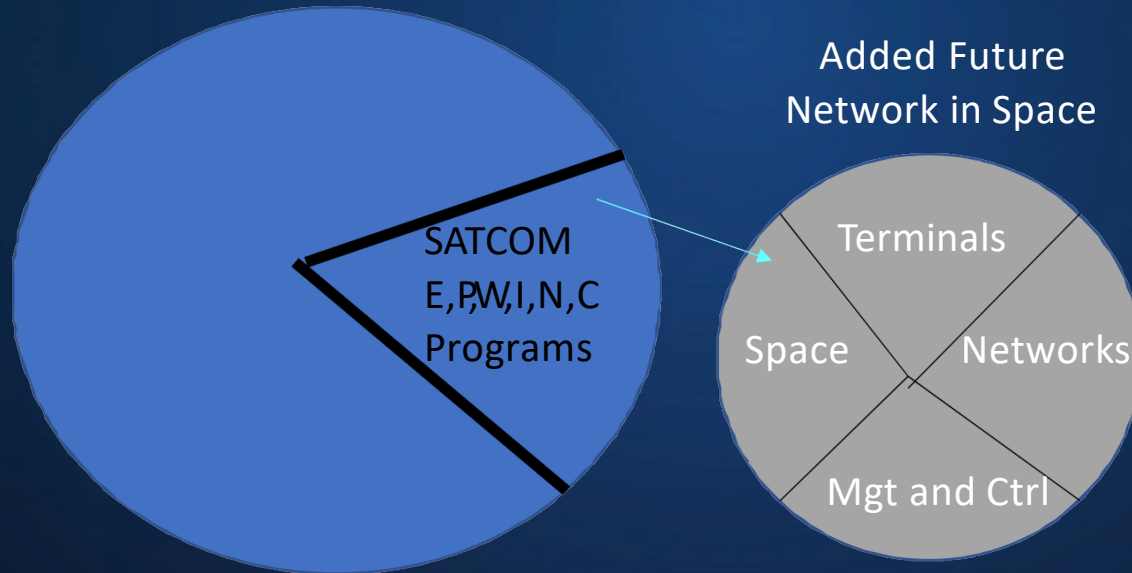
Interim National Security Strategic Guidance	2022 National Defense Strategy (NDS)	National Military Strategy (NMS)	2019 National Intelligence Strategy	National Cyber Strategy	National Strategy to Secure 5G	National Strategy to Secure Cyberspace	U.S. Intel Strategy for Cyberspace	United States Intelligence Community Information Sharing Strategy	2018 DoD Cyber Strategy
DoD Digital Modernization Strategy	DoD Cybersecurity Risk Reduction Strategy	DoD Artificial Intelligence Strategy (unless summary)	DoD Cloud Strategy	DoD Data Strategy	DoD Identity, Credential, and Access Management (ICAM) Strategy	DoD 50 Strategy	DoD Software Modernization Strategy	DoD Information Sharing Strategy	NIST Framework for Improving Critical Infrastructure Cybersecurity

ORGANIZE	ENABLE	ANTICIPATE	PREPARE	AUTHORITIES																		
<p>Design for the Fight</p> <p>NIST SP 800-119 Guidelines for the Secure Deployment of IaaS</p> <p>CSIA National Special Public Architecture Recommendations</p> <p>DoD O-5118-13 (CAC need) Critical Information Communications (CIRT/COM) System</p> <p>DoD 7046.20 Capacity PoM/Ms Management</p> <p>DoD 5000.02 Operation of the Adaptive Acquisition Framework</p> <p>DoD 5200.44 Protection of Mission Critical Functions to Achieve TSN</p> <p>DoD 8115.02 IT Portfolio Management Implementation</p> <p>DoD 8330.01 Interoperability of IT and National Security Systems (NSS)</p> <p>DoD 8501 Information Assurance (IA) in the Defense Acquisition System</p> <p>MOA between DoD CIO and OIG/CIO Establishing Non-Centric Software Licensing Agreement</p> <p>DTM 32-304 Building Cybersecurity Accountability of DoD Components and Information Systems</p> <p>CJCS 5123.01H Chapter of the JROC and Implementation of the JCID</p>	<p>Secure Data in Transit</p> <p>FIPS 140-3 Security Requirements for Cryptographic Modules</p> <p>CNSRP-11 Nati Policy Governing the Acquisition of IA and IaaS/Cloud IT</p> <p>CSIA Subpart 208.74 Enterprise Software Agreements</p> <p>CNSRP-17 Policy on Wireless Communications Protecting Nati Security Info</p> <p>CNSRP-28 National Policy for PDI in National Security Systems</p> <p>NAICS-2005 Communications Security (COMSEC) End Item Modification</p> <p>CNSI-5001 Type-Accommodation Program for VoIP Telephony</p> <p>NIST SP 800-102 Protected Distribution Systems (PDS)</p> <p>DoD 8521.01E Department of Defense Bonafide</p> <p>DoD 8100.04 DoD Unifed Capabilities (JC)</p> <p>DoD 8523.01 Communications Security (COMSEC)</p> <p>CJCS 8510.02E Cryptographic Modernization Plan</p>	<p>Understand the Battleground</p> <p>FIPS 193 Standards for Security Categorization of Federal Info and Info Systems</p> <p>NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories</p> <p>NISTIR 7800 Specification for Asset Identification 1.1</p> <p>CNSRP-29 Cybersecurity of Unimanned National Security Systems</p> <p>CNSI-6000 Voice Over Internet Protocol (VoIP) Computer Telephony Answer 1, VoIP/1</p> <p>NAICS-6002 National Policy for Protection of Govt Contractors' Telecommunications</p> <p>DoD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD OIG</p> <p>DoD 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum</p> <p>DoD 8420.01 Commercial WLAN Devices, Systems, and Technologies</p> <p>DoD 85200.16 Objectives and Min. Steps for COMSEC Measures used in NCI Control</p> <p>CJCS 8510.02E Cryptographic Modernization Plan</p>	<p>Prevent and Delay Attackers</p> <p>RFP 200 Minimum Security Requirements for Federal Information Systems</p> <p>NIST SP 800-37 R2 Security & Privacy Controls for Federal Information Systems & Orgs</p> <p>NIST SP 800-41 R2 Computer Security Incident Handling Guide</p> <p>NIST SP 800-128 R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise</p> <p>NIST SP 800-129 Data Integrity, Detecting & Responding to Alterations</p> <p>CNSI-1039 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)</p> <p>CNSI-1202E, Alpha 1-5 Security Overlays</p> <p>DoD 8500.01 Cybersecurity for Acquisition Decision Authority and Program Manages</p> <p>DoD 8205.01 DoD Insider Threat and Management and Analysis Center</p> <p>DoD 8531.01 DoD Vulnerability Management</p> <p>DoD O-8500.14M (CAC need) CIO Service Provider Certification and Accreditation Program</p> <p>DTM 17-007, Ch. 2, Defense Support to Cyber Incident Response</p> <p>CJCS 8510.01E Cyber Incident Handling Program</p>	<p>Develop and Maintain Trust</p> <p>CNSRP-12 National IA Policy for Space Systems Used to Support NSS</p> <p>CNSRP-21 National IA Policy on Enterprise Architecture for NSS</p> <p>NIST SP 800-160, Vol 1, Systems Security Engineering - Engineering of Trustworthy Secure Systems</p> <p>DoD 3030.40 Mission Assurance</p> <p>DoD 3100.10 Space Policy</p> <p>Strengthen Cyber Readiness</p> <p>NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems</p> <p>NIST SP 800-30, R1 Guide for Conducting Risk Assessments</p> <p>NIST SP 800-138, R3 SCAP Ver. 1.3</p> <p>IST DevSecOps Playbook to Guide the Federal Government</p> <p>CNSRP-32 Cloud Security for National Security Systems</p> <p>CNSI-5005 Supply Chain Risk Management</p> <p>DoD 3700.01 DoD Command and Control (C2) Enabling Capabilities</p> <p>DoD 8140.02 Identification, Tracking, and Engineering of Cyberthreat Workforce Requirements</p> <p>DoD 8500.01 Cybersecurity</p> <p>DoD 8560.01 COMSEC Monitoring</p>	<p>NATIONAL / FEDERAL</p> <p>Computer Fraud and Abuse Act Title 18 (§203)</p> <p>Stored Communications Act Title 18 (§2701 et seq.)</p> <p>Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)</p> <p>Executive Order 13526 Classified National Security Information</p> <p>Executive Order 13587 Structural Reforms To Improve Classified Info</p> <p>Executive Order 13636 Improving Critical Infrastructure Cybersecurity</p> <p>EO 13800 Strengthening Cybersecurity of Fed Nets and CI</p> <p>EO 13873 Securing the Information and Communications Technology and Services Supply Chain</p> <p>EO 14026 Improving the National Cybersecurity</p> <p>NSPD 54 / NSPD 23 Computer Security and Monitoring</p> <p>PPD 41: United States Cyber Incident Coordination</p> <p>PPD 28: Signals Intelligence Activities</p> <p>FAR Federal Acquisition Regulation</p> <p>Ethics Regulations</p> <p>JOE Special Access Program (SAP) Implementation Guide (JISG)</p> <p>NIST Special Publication 800-Series</p> <p>NIST SP 800-64, R1 Guidelines for Media Sanitization</p> <p>NIST SP 800-225A, R1 Security Recommendations for Hypervisor Platforms</p> <p>NIST SP 800-229 Security Guidelines for Storage Infrastructure</p> <p>NIST SP 800-503 National Directive On Security of National Security Systems (CNSI-4009)</p> <p>CNSI-4009 Critical on National Security Systems</p> <p>DoD Information Technology Environment Strategic Plan</p>																	
<p>Develop the Workforce</p> <p>NIST SP 800-181 R1 Workforce Framework for Cybersecurity</p> <p>CNSI-504 Protecting National Security Systems from Insider Threat</p> <p>CNSI-4000 Maintenance of Communications Security (COMSEC) Equipment</p> <p>CNSI-4012 National IA Training Standard for Senior Systems Managers</p> <p>CNSI-4014 National IA Training Standard for Information Systems Security Officers</p> <p>CNSI-4016 National IA Training Standard For Risk Analysts</p> <p>DoD 3035.09 Cryptologic Accreditation and Certification</p>	<p>Manage Access</p> <p>HSPC-12 Policy for a Common ID Standard for Federal Employees and Contractors</p> <p>NIST SP 800-210 General Access Control Guidance for Cloud Environments</p> <p>NIST SP 800-218 Securing Web Transactions, TLS Server Certificate Management</p> <p>CNSRP-10 Nati Policy Govt. Use of Approved Sec. Controls in Info System Applications</p> <p>CNSRP-20 National Policy on Controlled Access Programs</p> <p>CNSI-5006 National Directive for IAM Capabilities</p> <p>CNSI-1300 Instructions for NSS PDI X 509</p> <p>CNSI-4001 Operational Security Doctrine for the PDRFEZA User PDRGCA Card</p> <p>CNSI-4003 Reporting and Evaluating COMSEC Incidents</p> <p>CNSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSI-008-14</p> <p>DoD 1000.12 DoD Personal Identity Protection (PII) Program</p> <p>DoD 5000.08 Security of DoD Installations and Resources and the DoD PERB</p> <p>DoD 8521.01 Public Key Infrastructure (PKI) and Public Key (PK) Enabling</p> <p>DoD 8521.03 Identity Authentication for Information Systems</p> <p>DoD 5205.02 DoD Operations Security (OPSEC) Program Manual</p>	<p>Manage Access</p> <p>FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors</p> <p>NIST SP 800-181 Securing Web Transactions, TLS Server Certificate Management</p> <p>DoD 8531.01 DoD Vulnerability Management</p> <p>CNSI-5006 National Directive for IAM Capabilities</p> <p>CNSI-1300 Instructions for NSS PDI X 509</p> <p>CNSI-4001 Operational Security Doctrine for the PDRFEZA User PDRGCA Card</p> <p>CNSI-4003 Reporting and Evaluating COMSEC Incidents</p> <p>CNSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSI-008-14</p> <p>DoD 1000.12 DoD Personal Identity Protection (PII) Program</p> <p>DoD 5000.08 Security of DoD Installations and Resources and the DoD PERB</p> <p>DoD 8521.01 Public Key Infrastructure (PKI) and Public Key (PK) Enabling</p> <p>DoD 8521.03 Identity Authentication for Information Systems</p> <p>DoD 5205.02 DoD Operations Security (OPSEC) Program Manual</p>	<p>Sustain Missions</p> <p>NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems</p> <p>CNSRP-18 National Policy on Classified Information Storage</p> <p>DoD 8551.01 National Policy on Control of Compromising Emissions</p> <p>CNSI-4004A, 1, Description and Elements Protection Procedures for COMSEC and Class. Material</p> <p>CNSI-7000 TEMPEST Guidelines for Facilities</p> <p>DoD 3020.26 DoD Continuity Policy</p> <p>DoD 8144.02 DoD Chief Information Officer</p> <p>DoD 8000.03 Technology & Program Protection to Maintain Technological Advantage</p> <p>ICJ 903 IT Systems Security Risk Management and CIA</p> <p>NSA IA Directive (IAD) Management Directive MD-110 Cryptologic Key Protection</p>	<p>OPERATIONAL/SUBORDINATE POLICY</p> <p>CYBERCOM Orders</p> <p>Security Configuration Guide (SCOG)</p> <p>NSA IA Guidance</p> <p>JFMC-DODM Orders</p> <p>Companioned Joint Policy (Directive, Security, Posture, Memoranda)</p> <p>Security Technical Implementation Guide (STIG)</p>																		
<p>Partner for Strength</p> <p>NIST SP 800-144 Guidelines on Security and Privacy in Public-Cloud Computing</p> <p>NIST SP 800-172A Enhanced Security Requirements for Providing Cloud</p> <p>CNSI-4008 Program for the Mgt and Use of Nati Reserve IA Security Equipment</p> <p>DoD O-5205.13 DoD CISA Program Security Classification Manual (NSFCOM)</p> <p>Cybersecurity Maturity Model Certification (CMMC)</p>	<p>Assure Information Sharing</p> <p>CNSRP-04 Policy on Assured Info Sharing (AIS) for National Security Systems (NSS)</p> <p>DoD 8100.01 Sharing Data, Info, and IT Services in the DoD</p> <p>CJCS 3213.01D, Joint Operations Security</p> <p>DoD 8170.01 Online Information Management and Electronic Messaging</p> <p>DoD 8182.01 Security of Non-DoD Info Sys Providing Unrestricted Nonpublic DoD Information</p> <p>CJCS 6111.02D Defense Information System Network (DISN) Responsibility</p>	<p>Partner for Strength</p> <p>NIST SP 800-171, IC Protecting CUI in Nonfederal Systems and Organizations</p> <p>CNSRP-14 National Policy Governing the Release of IA Products/Services</p> <p>DoD 5005.13 Defense Industry Base (DIB) Cyber Security (CI) IA Activities</p> <p>DoD 5220.23 M, Ch. 2 National Industrial Security Program Operating Manual (NISCOM)</p> <p>DoD 8200.01 DoD 8200.01</p> <p>MOA Between DoD and DHS (Jan. 19, 2017)</p>	<p>ABOUT THIS CHART</p> <p>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 linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.</p> <p>CNSI policies link only to the CNSI site. Boxes with red borders represent recent updates.</p> <p>*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.</p> <p>For the latest version of this chart or email alerts to updates go to updates@csiac.org.</p>	<p>Color Key - OIDs</p> <table border="1"> <tr> <td>DoD OIG</td> <td>NIST</td> <td>USRMS</td> </tr> <tr> <td>CNSI/NSS</td> <td>NSA</td> <td>USRP</td> </tr> <tr> <td>DNA</td> <td>OSD</td> <td>USDP/AFJ</td> </tr> <tr> <td>DS</td> <td>CYBERCOM</td> <td>Other Agencies</td> </tr> <tr> <td>JAP</td> <td>USRAAS</td> <td>Recently updated policy and/or update, unless pending</td> </tr> <tr> <td>NSA IA Directive (IAD) Management Directive MD-110 Cryptologic Key Protection</td> <td>USDC</td> <td></td> </tr> </table>	DoD OIG	NIST	USRMS	CNSI/NSS	NSA	USRP	DNA	OSD	USDP/AFJ	DS	CYBERCOM	Other Agencies	JAP	USRAAS	Recently updated policy and/or update, unless pending	NSA IA Directive (IAD) Management Directive MD-110 Cryptologic Key Protection	USDC	
DoD OIG	NIST	USRMS																				
CNSI/NSS	NSA	USRP																				
DNA	OSD	USDP/AFJ																				
DS	CYBERCOM	Other Agencies																				
JAP	USRAAS	Recently updated policy and/or update, unless pending																				
NSA IA Directive (IAD) Management Directive MD-110 Cryptologic Key Protection	USDC																					

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

Space Networking Decomposed

Space Systems Enterprise



Space Networks

- 40 Operators
- 150 terminal types
- 200K users
- 100s of networks supported
- 10 Types of Mgt and Control