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 | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Welcome and Introduction

James McCarthy, NCCOE

08/11/2022

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

NIST CSF Profiles

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

NIST CSF Profiles

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
	Improvements	RS.IM
Recover	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

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SSC Intro

Joe Vanderpoorten, NH-04

SATCOM Technical Director

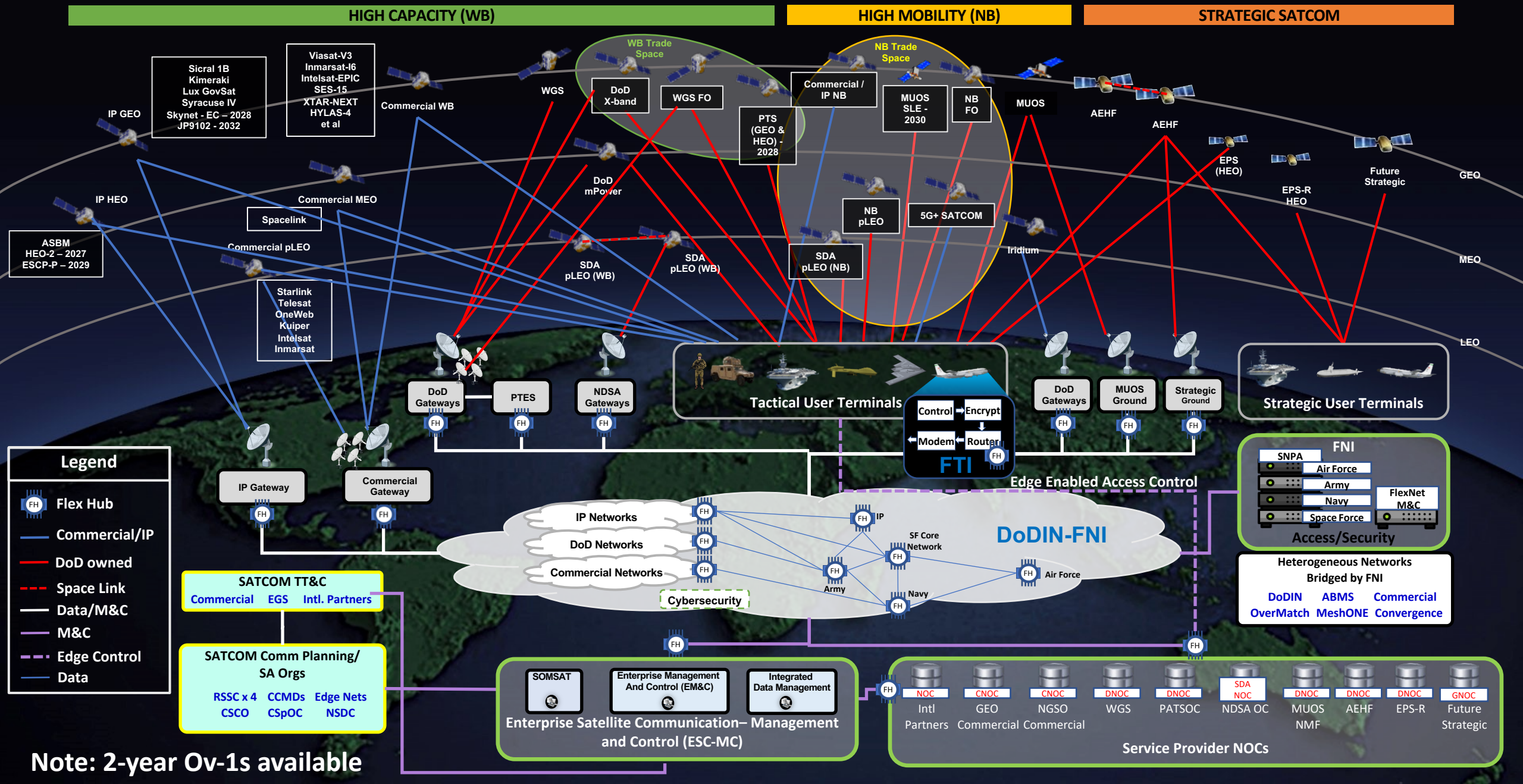
PEO for SATCOM and Navigation

Space Systems Command

US Space Force

Joseph.Vanderpoorten@spaceforce.mil

SATCOM Hybrid Architecture (2032) OV-1



Note: 2-year Ov-1s available

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

Enterprise Level Threat
Enterprise Level Response

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

AISR Tech Roadmap

Problem

Sophisticated Enterprise Attack – Need AISR Enterprise Response?

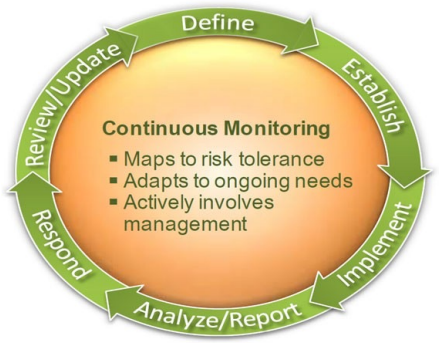
Generic Threat Visualization Actuals

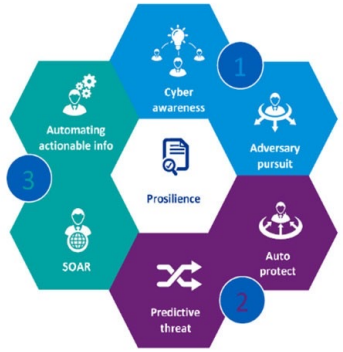
Primary Space Cyber Threats

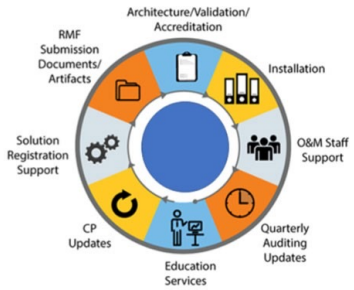
Threat	Description	Insertion Points	Mitigations	Metadata/Metric
DOS/DDOS and associated attacks	Denial of Service Attacks or Distributed Denial of Service (DDoS) attacks are much concern to the SATCOM industry. Mostly effecting terrestrial nodes.	Boundary equipment	NextGen Firewalls utilizing Advanced 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.

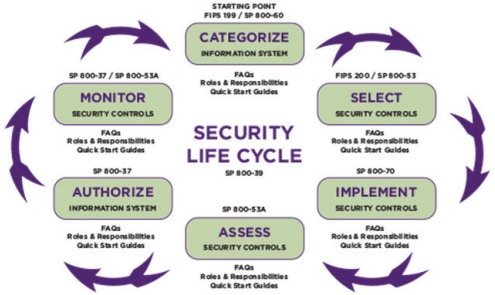
*Note: The list above is not exhaustive. Other methods of mitigation are to implement a Zero Trust Architecture (ZTA) and the utilization of new cryptography like quantum encryption.

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

Notional Cyber Strategy

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

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

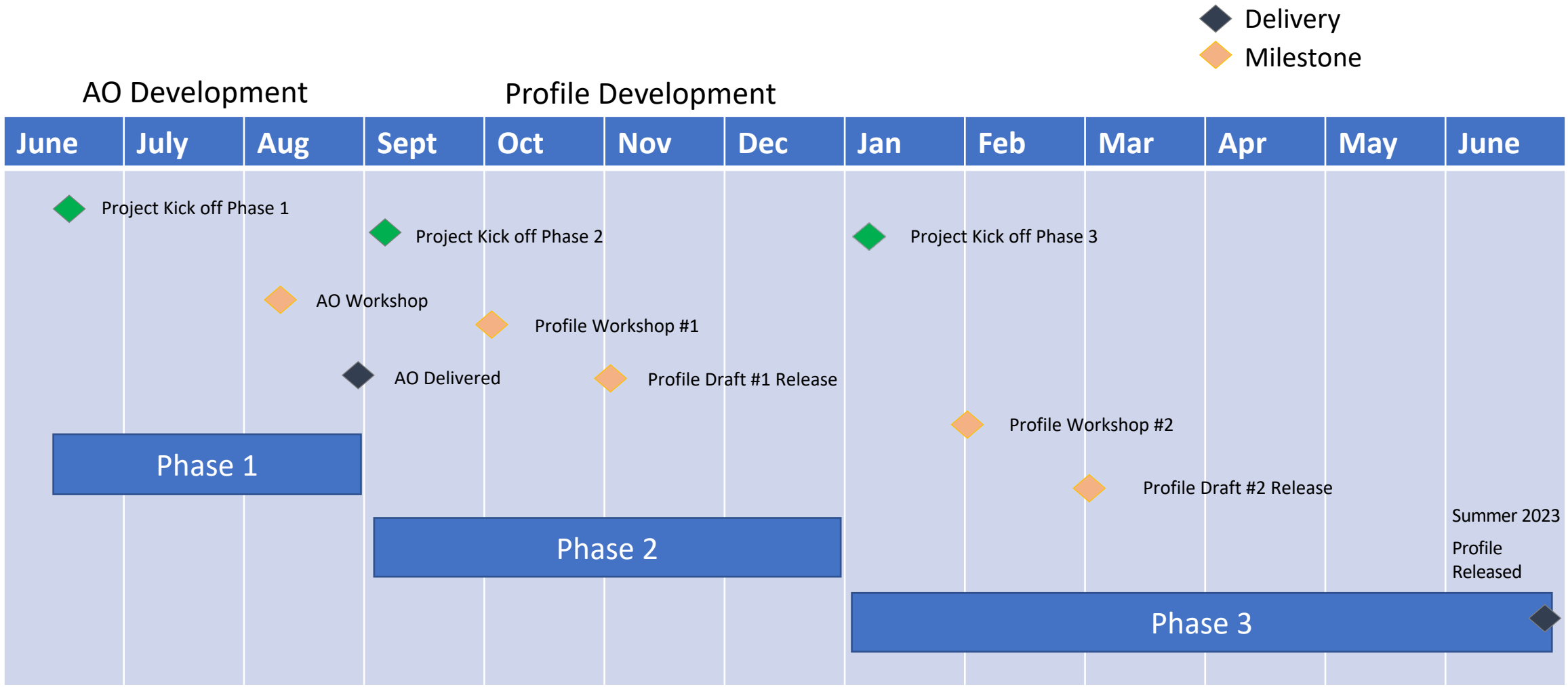
Background and Purpose: HSN Cybersecurity

- 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



HSN Annotated Outline

Overview and Comment Review

Joe Brule/ MITRE

08/11/2022

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

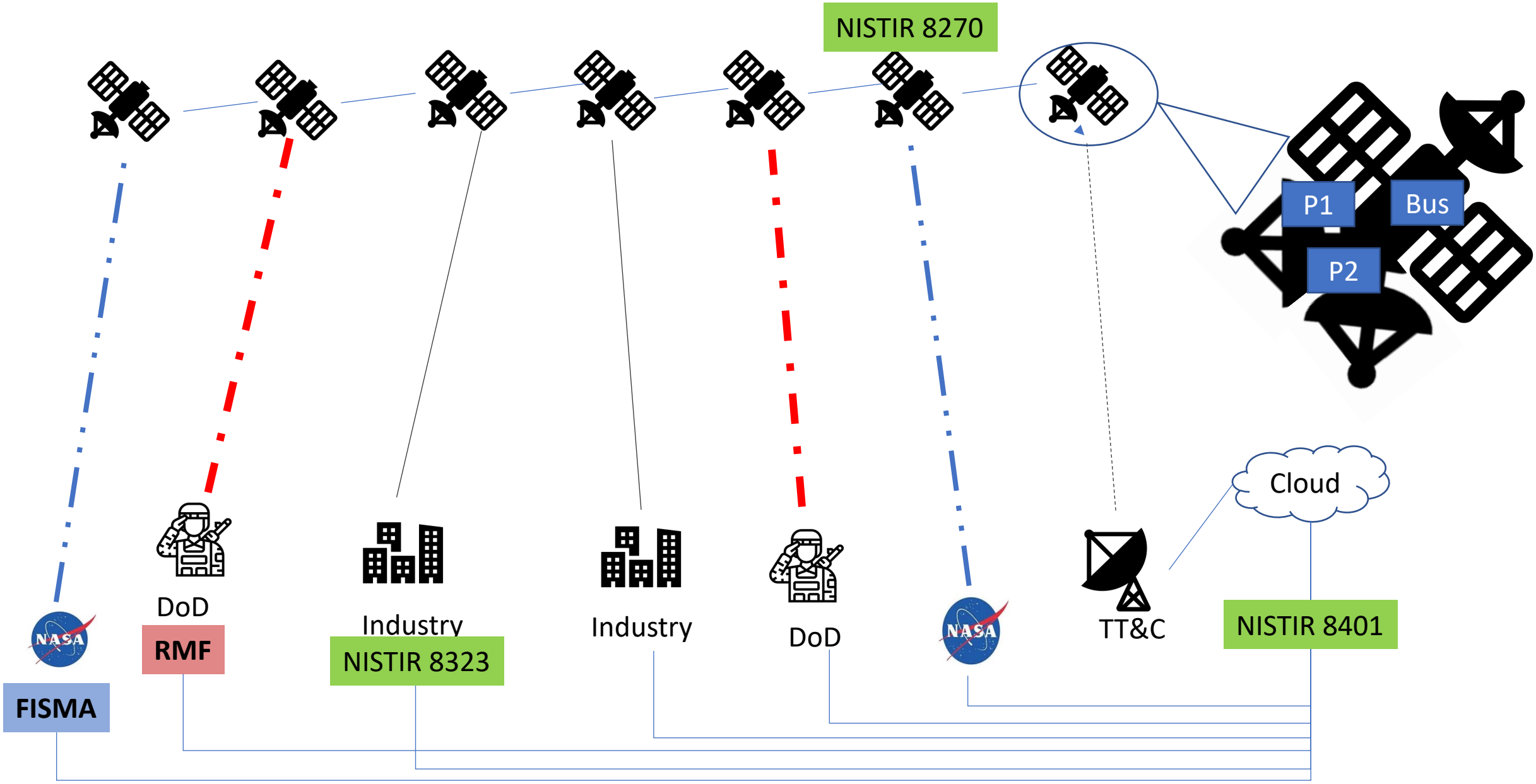
CSF language

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.

AO Comment Review

- 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

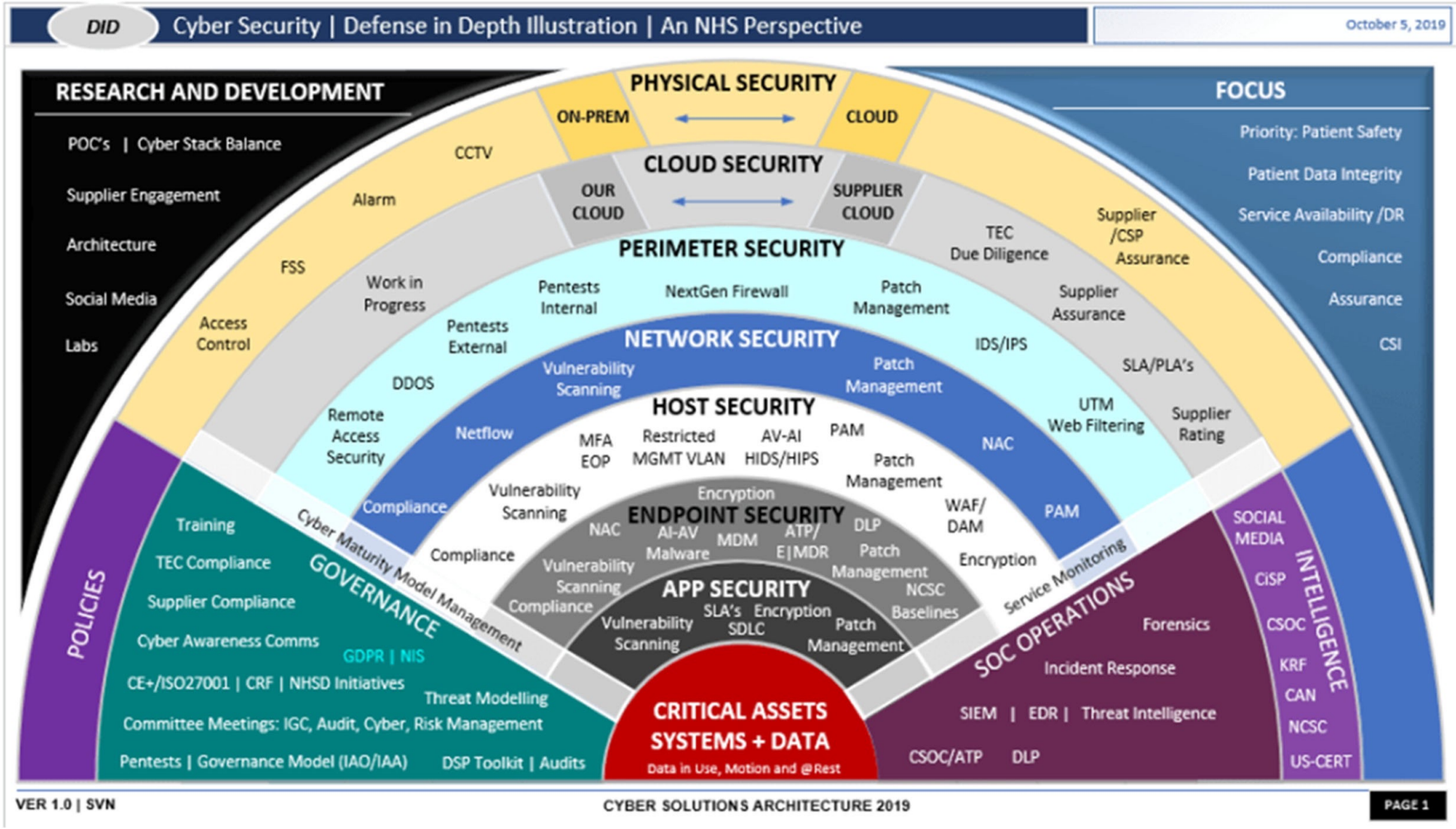

NISTIR 8270
P1
Bus
P2
Cloud
DoD
RMF
Industry
NISTIR 8323
Industry
DoD
TT&C
NISTIR 8401
FISMA

HSN Community of Interest

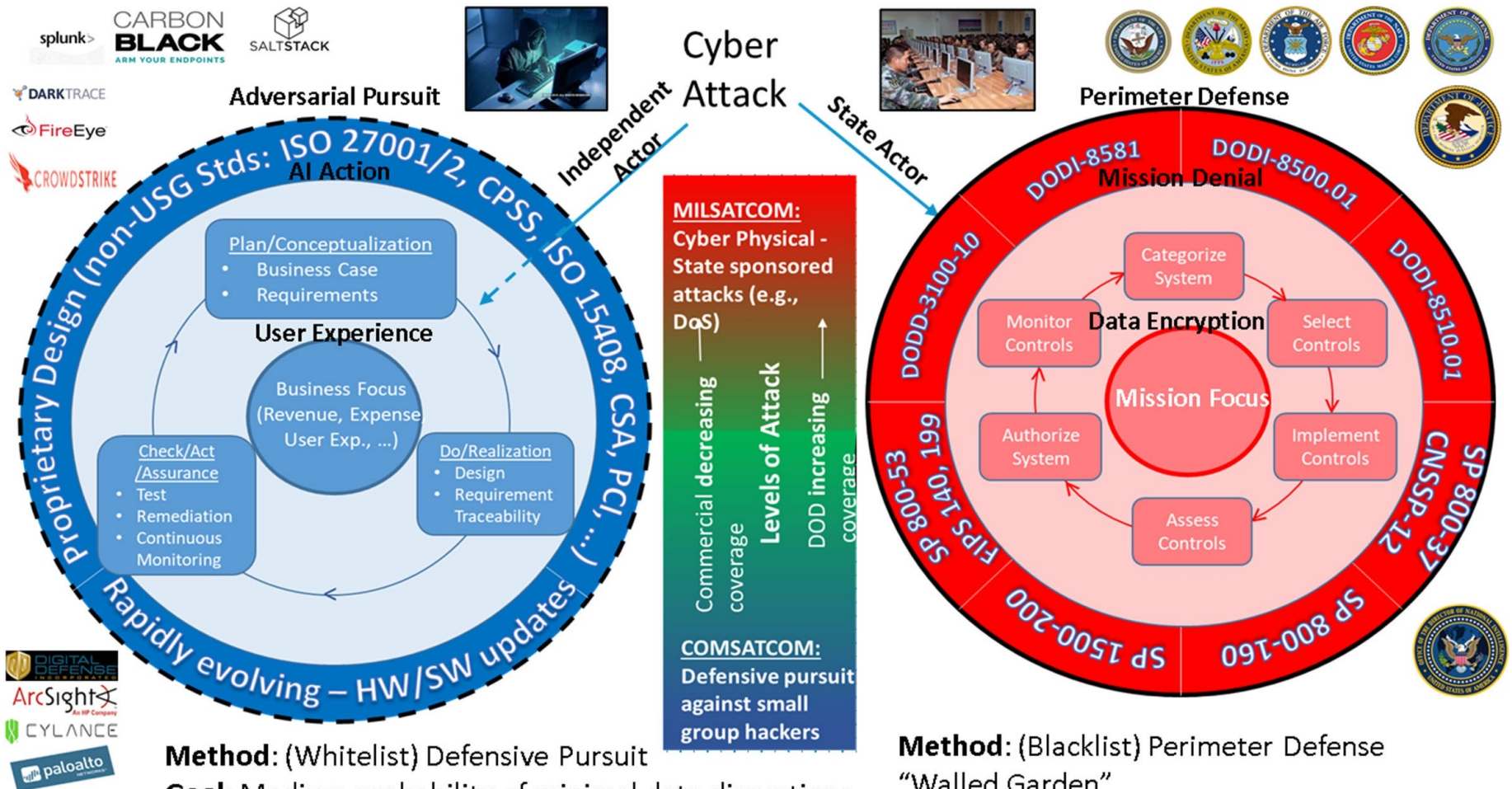
- Community Driven Effort to Produce a Draft
- Tempo
  - Biweekly Web-conferences
  - Comment submission/ resolution between meetings
  - Optional Deep Dives
- Members
  - Satellite Operators
  - Satellite Vendors
  - Government
  - Academia
  - Consultants
- Join by Contacting HSN COI (Currently 35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

Backups

Defense-in-Depth



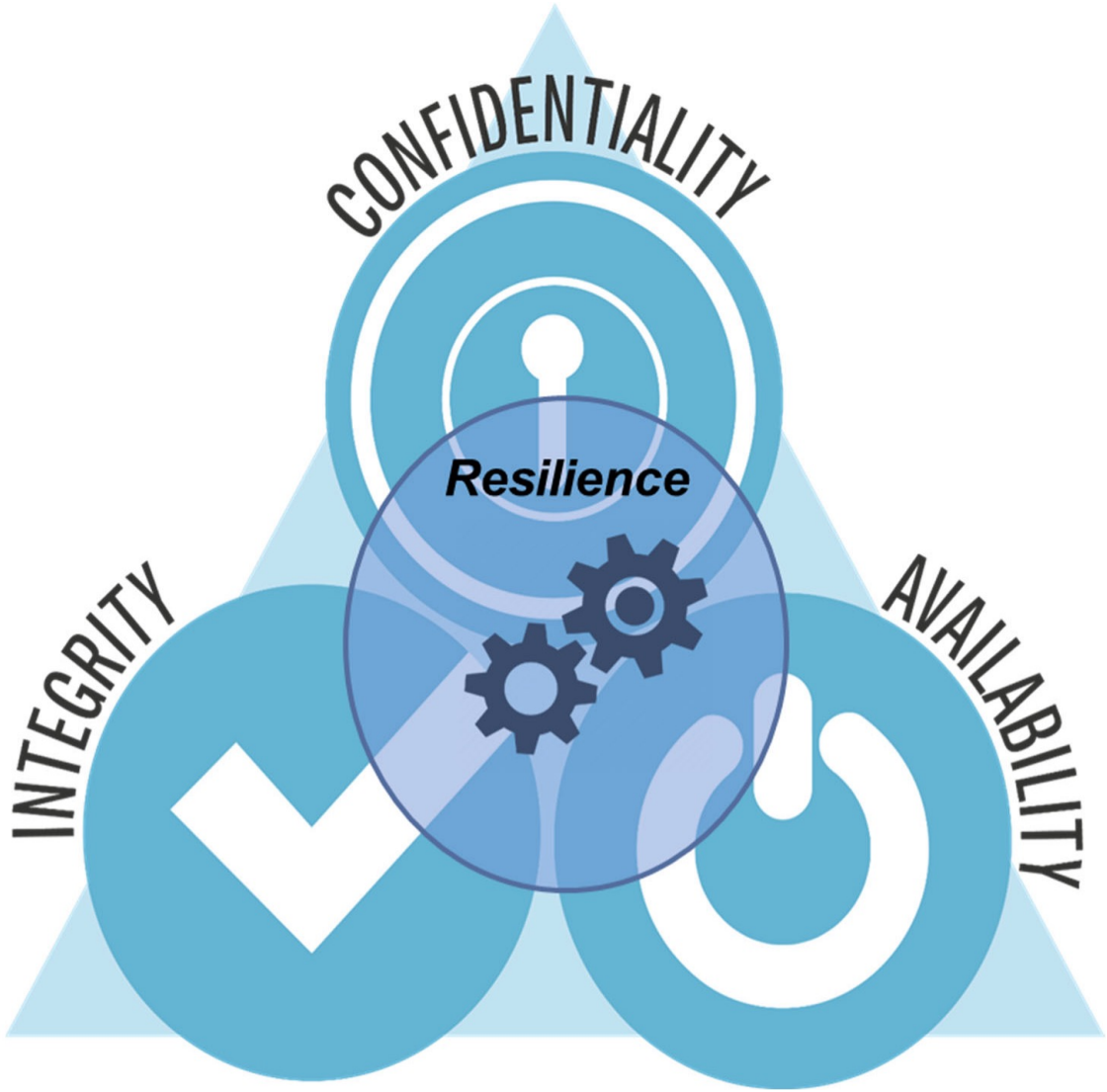
COMSATCOM v. MILSATCOM



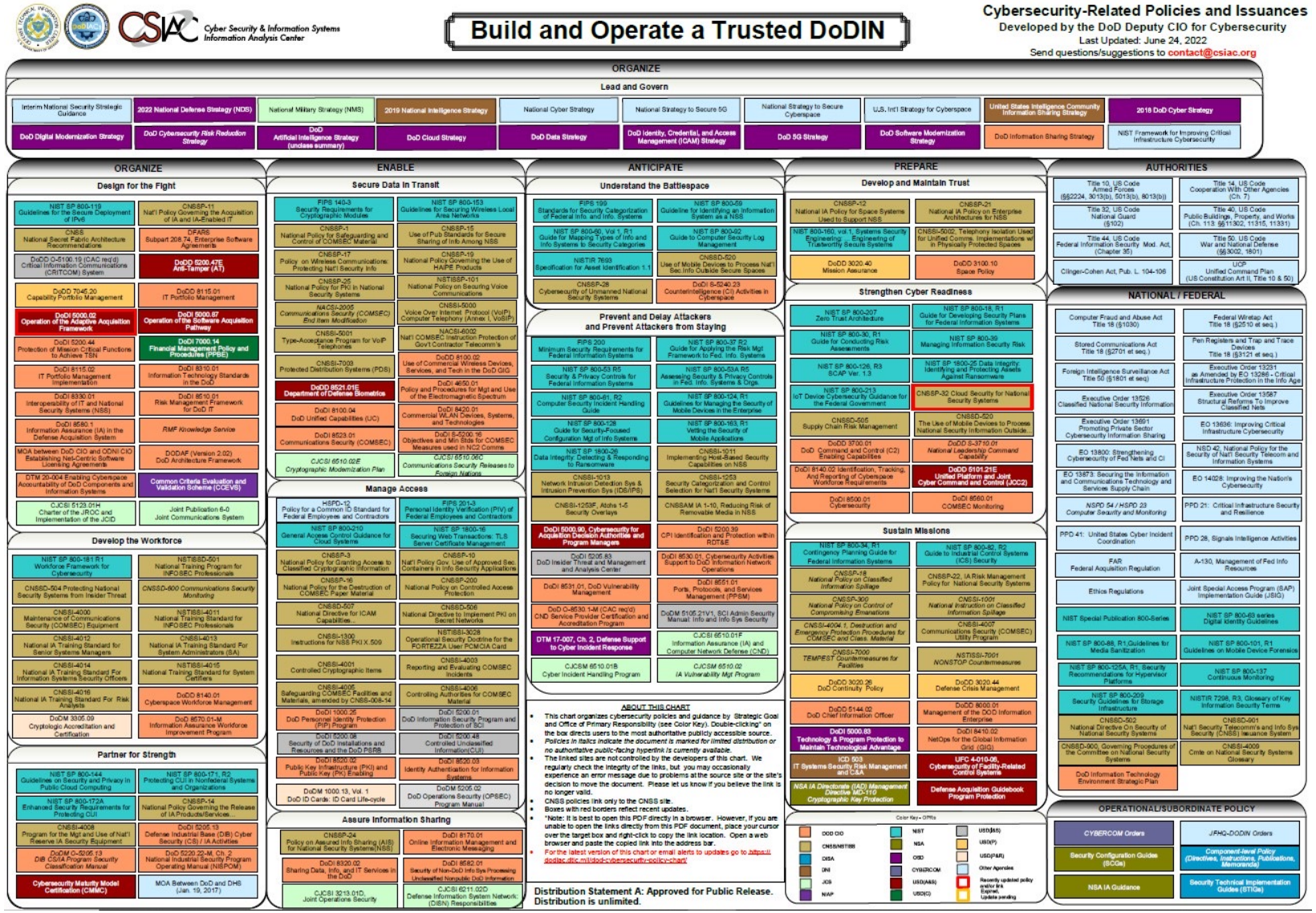
Method: (Whitelist) Defensive Pursuit
Goal: Medium probability of minimal data disruptions, high situational awareness and system integrity.
Issue: Less secure boarder to insure user experience

Method: (Blacklist) Perimeter Defense "Walled Garden"
Goal: High probability of mission success!
Issue: Lack of insight and maintenance.

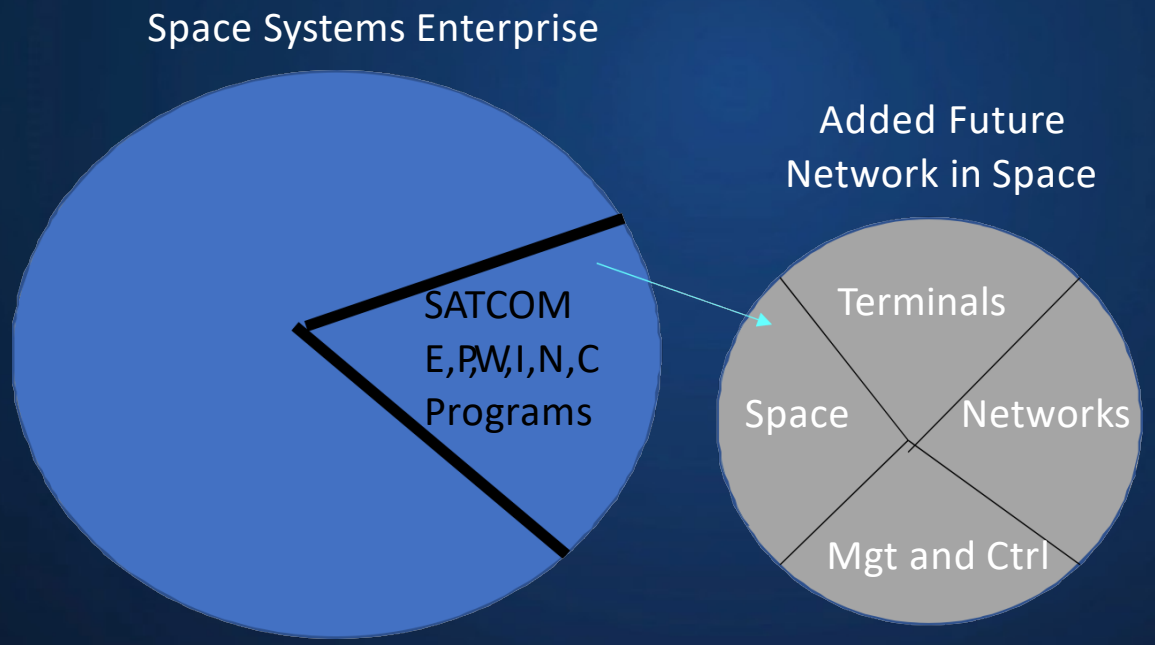
Overlap of CIA = Resilience



Navigating and Adhering to Complex Policies



Space Networking Decomposed



Space Networks

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