National Institute of Standards and Technology
U.S. Department of Commerce

NIST IR 8401 (DRAFT)

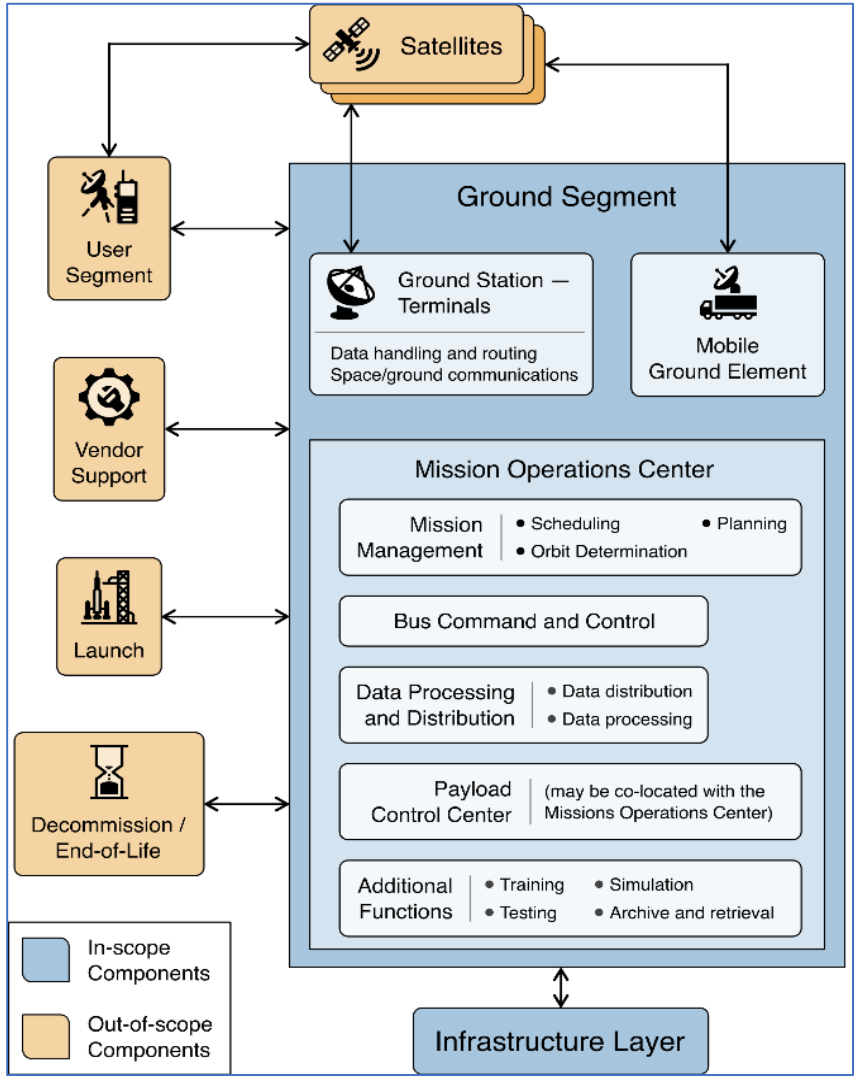
Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control

Jim McCarthy/ NIST

Joe Brule/ MITRE

06/16/2022

NISTIR 8401 Scope



- NISTIR 8401: Ground Segment
  - Terminals
  - Mission Operation Centers
  - Payload Operation Centers
- Separate NISTIRs for Other Segments
  - User Segment (NISTIR 8323)
    - Update underway
  - Space Vehicle (Draft NISTIR 8270)
    - Resolving Comments Now

Background: Ground Segment Profile

- SPD 5, Protecting American Space Systems from Cyber Threats: "… directs U.S. Government agencies to work with commercial companies consistent with the principles in the SPD to further define best practices, establish cybersecurity informed norms, and promote improved cybersecurity behaviors throughout the Nation's industrial base for space systems"

- Space Systems Center (SSC) Statement of Work;

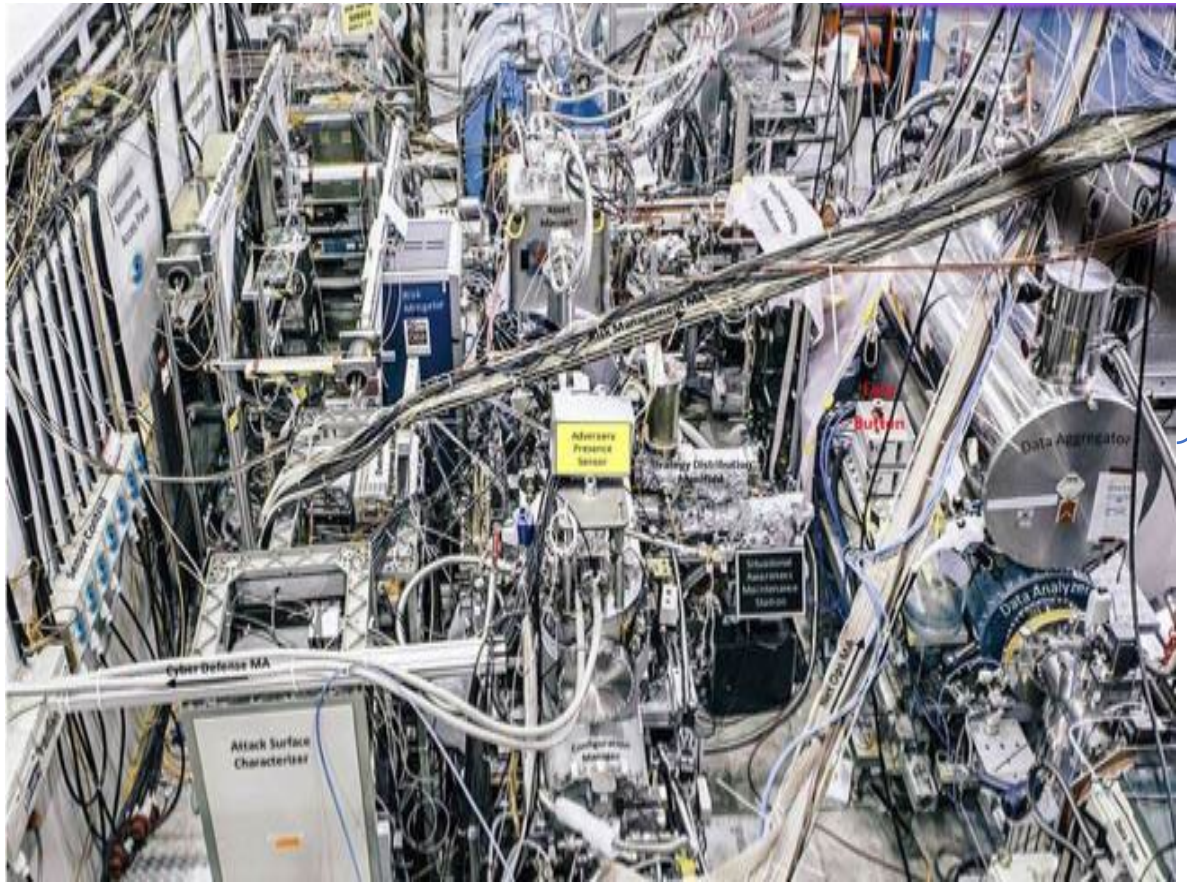
  "… In addition, SSC is seeking **diversity of perspective** especially with regards to our civilian user communities and their requirements and needs."

  - CSF Profile development enabled SSC to gain commercial perspective
    - How does industry address cybersecurity issues?
    - What is the residual risk to Commercial Space?
  - The resulting CSF Profile will help the commercial satellite industry improve their cybersecurity posture
  - Greater Sector Security Contributes to Hosted Payload Risk Analysis

NISTIR 8401 Development

- SSC Statement of Work:
  - Collaborate with NIST NCCOE
  - SSC GPS office provided FFRDC support
  - Develop a Cyber Security Framework (CSF) Profile for Satellite Ground Systems
- The Approach
  - NIST Hosts Workshop/Engage Industry
  - Solicit Participation in a “Community Of Interest”

Facilitating Cybersecurity Discussions



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

Content of a Sector Level Profile

Guidance on how to apply the subcategory to the space ground segment

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.

Leveraging Industry

- NIST Hosted Multiple Workshops
  - CSF Overview
  - Introduce Ground Segment Profile
  - Solicit Participation in a “Community Of Interest”
  - ‘Chatham House Rules’
  - Draft Sections and resolve comments

Date	Session	Purpose
24 JUN 2021	Workshop	Introduce the CSF to industry
23 SEP 2021	COI Meeting	Front Matter
7 OCT 2021	COI Meeting	Identify Function
21 OCT 2021	COI Meeting	Protect Function
4 NOV 2021	COI Meeting	Detect Function
18 NOV 2021	COI Meeting	Respond and Recover Functions
18 NOV 2021	Deep Dive	Remote access and cloud
22 NOV 2021	Deep Dive	Ground Infrastructure as a service
2 DEC 2021	COI Meeting	End-to-End Review

Industry Actively Participated in the Creation of this Profile.

Community of Interest

- ~ 130 Members representing over thirty organizations
  - Satellite Vendors, Operators, Government, Academia,
  - Consultants, Private Individuals, Cloud Service Providers

Key Finding: Movement to Cloud

- Virtualization
  - Virtual Machines and Environments
    - Flexible, facilitates testing, system administration, recovery
    - Permissions based on RBAC (vice access to specific hardware)
    - Challenges/ Considerations
      - May need to augment authentication/ authorization
      - Device authentication
      - Hypervisor considerations such as VM escape
  - Smaller satellite operators are more likely to adopt cloud based providers
  - Cloud is most suitable for commodity hardware/ software.
  - Critical Satellite bus commands are still done from a dedicated SOC
  - Requires aggressive monitoring to verify that all activity is authorized and within the terms of pre-defined agreements
- Zero Trust, Machine Learning, Artificial Intelligence
  - Considered futuristic
  - Being monitored
  - Not ready to adopt in the immediate future

Key Finding: Increased Decoupling of Segments

- Federated Infrastructure
  - Fewer Dedicated Operations Centers
  - Ground site as a service
  - Distributed Antenna fields (queued commands)
  - Distributed Mission and Satellite Operation Centers
  - Isolation of flows done in parallel (vice double encryption within tunnels)
- Less Reliance on Physical Protection Measures
  - Less reliance on Air Gapping
    - External data flows (ex. planning, collision avoidance etc.) inhibited by air gapping.
  - More focus authentication mechanisms

Key Findings: CSF Functions (One of three)

- Identify
  - Payload Command Centers, Mission Operation Centers, Ground sites may be independent organizations or provided as a third-party service.
  - Identification of roles, responsibilities, terms of service must be identified and agreed upon in advance on a case-by-case basis.
  - Data Separation, access and authorization are determined in advance on a case-by-case basis.
  - Multiple Organizations may interface with the satellite platform resulting in very complex authentication/ authorization interfaces.
- Protect
  - Space uses custom software and hardware
    - Legacy systems are not always suitable for highly interconnected cyber-ecosystem.
    - Additional considerations warranted for niche components
    - Vendor support (for specialized components) require remote access for maintenance.

Key Findings: CSF Functions (Two of three)

- Detect:
  - Severe SWaP constraints of space vehicle will impact Ground Segment's detection requirements
  - Incumbent on Ground Segment to consider third party stakeholder's (such as hosted payload) requirements and constraints
  - Standards-based solutions for data formatting, and transmission facilitates interoperability, integration and sharing.
  - Attributes such as criticality, sensitivity, tolerance to false positives etc. will vary amongst stakeholders. The setting and review of thresholds need to be agreed upon on a case-by-case basis in advance.
  - Detection attributes are influenced by the risk assessment
  - Include the continuous monitoring of the RF environment
  - Detection information is shared with stakeholders or regional organizations to facilitate collaboration

Space operations use custom software and hardware that did not necessarily consider the environment of a highly interconnected cyber-ecosystem. This can be especially problem

Key Findings: CSF Functions (Three of three)

- Respond/ Recover
  - Situational awareness is key for appropriate and timely response and recover
  - Exchange information with external stakeholders and providers in accordance with pre-arranged agreements and thresholds is paramount to respond and recover
  - The investigation of RFI may involve and in some cases require notification of external agencies.

Way Forward

- Current Profiles
  - Ground Segment (Draft NISTIR 8401)
    - Public comment period open until; 06/21/2022
    - Please submit comments to; pnt-eo@list.nist.gov
    - Final document expected Q4 FY2022
  - User Segment (NISTIR 8323 Rev. 1 Draft Upcoming)
    - Release for public comment; June 2022
    - Final document expected Q1 FY2023
  - Space Vehicle (Draft NISTIR 8270)
    - Comment period closed; 04/08/2022
    - Comment adjudication underway and final document TBD

- Possible Future Profiles
  - Launch Profile
  - Transfer Profile
  - IMINT Profile
  - Satellite Internet Service Provider Profile

Thank you!

Profile Links

- NISTIR 8401 (Draft), Satellite Ground Segment: Applying the Cybersecurity Framework | CSRC
- NISTIR 8323, Foundational PNT Profile | CSRC
- NISTIR 8270 (Draft), Intro to Cybersecurity for Commercial Satellite Operations | CSRC

Contact Information

- pnt-eo@list.nist.gov
- Joseph.Brule@nist.gov
- Suzanne.Lightman@nist.gov
- James.McCarthy@nist.gov
- Matthew.Scholl@nist.gov