National Aeronautics and
Space Administration

Mission Resilience and Protection Program Status Update and Engineering Cybersecurity: Continuing the Conversation

Presented to the GSFC Systems Engineering Seminar

December 8, 2020

Joshua.Krage@nasa.gov

NASA Office of the Chief Engineer
Mission Resilience and Protection Program

Today's Discussion

Part One:

- Information and status on the Mission Resilience and Protection Program

Part Two:

- Advocating for cybersecurity as a core element of engineering
  - Primarily as a sub-discipline: systems security engineering
- Establishing a systems security engineer for each project
- …starting with some background to establish context

Mission Resilience and Protection Program

Mission Resilience and Protection

Goal

- Support space flight and support systems in improving resilience and protecting from the effects of malicious threat actors.

Brief History

- Established under OCE in 2012 as the Space Asset Protection Program (SAPP). Renamed to the Mission Resilience and Protection Program (MRPP) in March 2020.
- Supported by and chaired the Space Protection Working Group (SPWG), chartered under the APMC in 2012 to:
  - *"…ensure the resilience of mission-essential functions enabled by civil spacecraft and their supporting infrastructures against intrusion, disruption, degradation, and destruction, whether from environmental or hostile causes."*
  - SPWG charter allowed to lapse in 2018.
- NASA Principal Advisor for Enterprise Protection (EP), and associated Enterprise Protection Program (EPP) established in 2016 to address intra-discipline/organization protection challenges
  - MRPP is a core supporting element to the overall EP program
- Core competency support organizations exist within HEOMD (System Protection Office at JSC), SMD (lead for EP and Cybersecurity), GSFC (599/System Engineering's SAPP team), and JPL (Mission Protection Office)

Threats From Malicious Actors

Defense Intelligence Agency:

With sophisticated knowledge of satellite [command and control] C2 and data distribution networks, actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems, associated ground infrastructure, users, and the links connecting them.

Defense Intelligence Agency (DIA); Report Number: DIA_F_01403_A;
Date of Publication: February 2019; Report Title: Challenges to Security in Space;
URL:
https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

Counterspace Continuum
Modeling the types and means of counterspace threats

Source: National Air and Space Intelligence Center (NASIC)

Specific Threat Areas to Consider

Spacecraft Command Link

- Inadvertent interference on command link frequencies
- Purposeful interference / jamming
- Purposeful probing of the receiver, unauthorized command attempts

GPS / GNSS

- Jamming/denial of the GPS signals
- Measurement or data spoofing of GPS signals

Cybersecurity

- Command link bypass/subversion, e.g., operations console hijack
- Re-purposed sub-systems on the space platform
- Loss of critical digital reference files, e.g., via ransomware

Directed Energy

- Saturation of or damage to optical sensors from excess energy

Specific Threat Areas to Consider

Spacecraft Command Link

- Inadvertent interference on command link frequencies
- Purposeful interference / jamming
- Purposeful probing of the receiver, unauthorized command attempts

Observed

GPS / GNSS

Observed

- Jamming/denial of the GPS signals
- Measurement or data spoofing of GPS signals

Cybersecurity

Access obtained

- Command link bypass/subversion, e.g., operations console hijack
- Re-purposed sub-systems on the space platform
- Loss of critical digital reference files, e.g., via ransomware

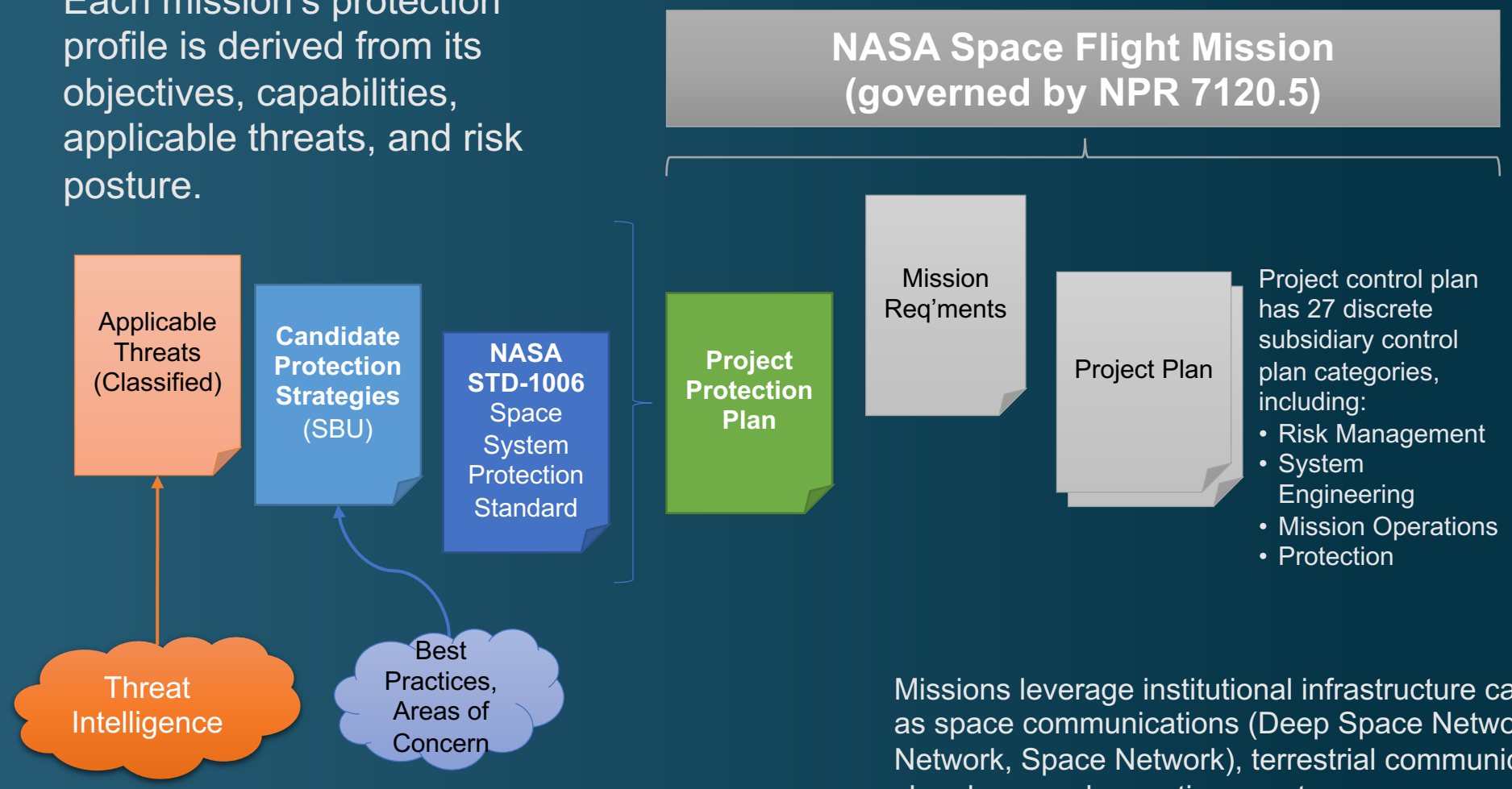
Observed

Directed Energy

- Saturation of or damage to optical sensors from excess energy

Space Protection Approach

Each mission's protection profile is derived from its objectives, capabilities, applicable threats, and risk posture.



Missions leverage institutional infrastructure capabilities, such as space communications (Deep Space Network, Near Earth Network, Space Network), terrestrial communications, test chambers, and operations centers.

Recent MRPP Activities

Policies and guidance

- Issued NASA-STD-1006 *Space System Protection Standard w/Change 1*
- Policy updates to support NASA-STD-1006, improve guidance
  - NID 1058.127, NPR 7120.5 (change 18), NPR 7120.8 (update)
- Updated Candidate Protection Strategies (v4), next version pending
- Updated Project Protection Plan template (streamlined), update pending

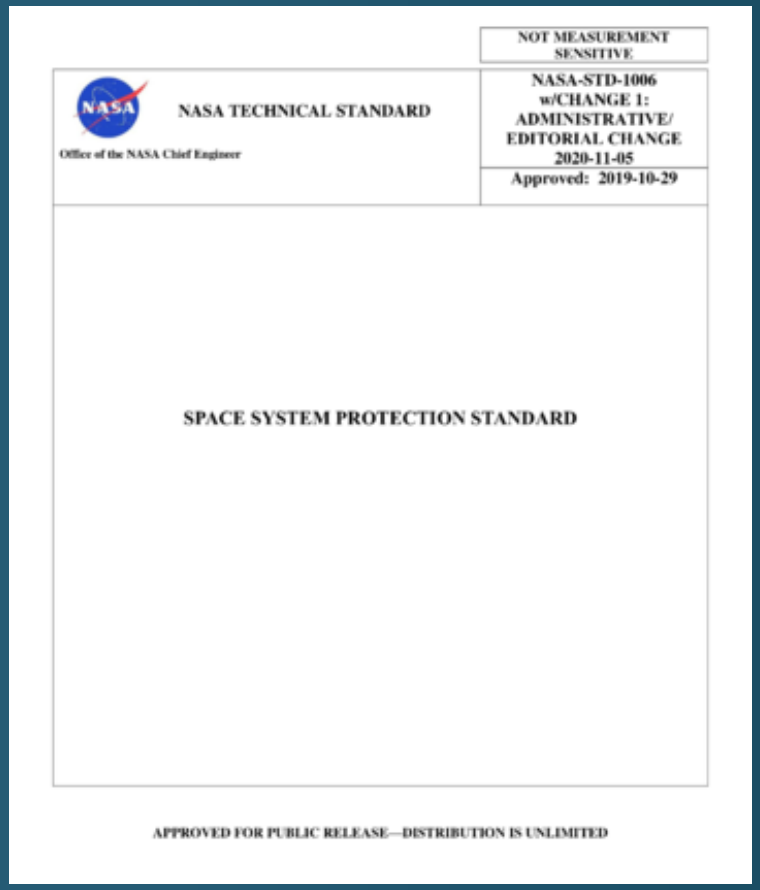
Experiments

- End-of-mission tests

Intra-organization collaboration

- OCIO: cybersecurity, supply chain
- OPS/Intel: analysis and threat briefings (NEW: unclassified threat briefing)
- OSMA: supply chain, mission vulnerabilities (IV&V)
- GSFC, JPL, SMD: deep space mission protection, cryptographic guidance
- HEO (SCaN, SPO): PNT topics, threat mitigation

NASA Technical Standard NASA-STD-1006 **w/ Change 1**
Space System Protection Standard [approved 2019-10-29, updated 2020-11-05]



NOT MEASUREMENT SENSITIVE

NASA TECHNICAL STANDARD

Office of the NASA Chief Engineer

NASA-STD-1006 w/CHANGE 1: ADMINISTRATIVE/ EDITORIAL CHANGE 2020-11-05

Approved: 2019-10-29

SPACE SYSTEM PROTECTION STANDARD

APPROVED FOR PUBLIC RELEASE—DISTRIBUTION IS UNLIMITED

NID 1058.127 directs use of NASA-STD-1006 in all programs/projects started after February 1, 2019. Existing programs/projects should discuss with MRPP which elements to address.

Highlighted phrases are updates from the prior version

Maintain Command Authority

- Command Stack Protection: Programs/projects shall protect the command stack with encryption that meets or exceeds the FIPS 140, Level 1.
- Backup Command Link Protection: If a project uses an encrypted primary command link, any backup command link shall at minimum use authentication.
- Command Link Critical Program/Project Information (CPI): The program/project shall protect the confidentiality of command link CPI as NASA SBU information to prevent inadvertent disclosure to unauthorized parties per NASA NID 1600.55 and NPR 2810.1.

Ensure Positioning, Navigation, and Timing (PNT) Resilience

- PNT Interference Recognition: If project-external PNT services are required, projects shall ensure that systems are resilient to the complete loss of, or temporary interference with, external PNT services.

Report Unexplained Interference

- Interference Reporting: Projects/Spectrum Managers/Operations Centers shall report unexplained interference to MRPP or to other designated notifying organizations.
- Interference Reporting Training: Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.

https://standards.nasa.gov/standard/oce/nasa-std-1006-wchange-1

Protection Plan Content Breakout

Protection Plan

- Project/mission background
- Protection-related requirements
- Susceptibilities
- Risk assessment
- NASA-STD-1006 assessment
- Candidate Protection Strategies assessment

Plan is normally controlled as NASA Sensitive But Unclassified (SBU).

Appendix

- Threat applicability
- Threat summary
- Vulnerability analysis
- Detailed risk analysis
- Mitigation recommendations

Appendix is normally Classified due to content.

Current template is available on the MRPP CoP on the NEN: https://nen.nasa.gov/web/sap/

Candidate Protection Strategies (CPS) v4

- The strategies serve as a starting point for mission protection planning
- Best practices, consider relevant threat intelligence and risk issues
- Protection plans incorporate results of the CPS analysis, including any requisite requirement tailoring

CPS document is NASA Sensitive But Unclassified (SBU), available:
- via the NASA Engineering Network (NEN) MRP community of practice site (in the SBU folder), or
- via request from the NASA MRPP team

Main Categories (# of questions)

1. Engineering Focused Strategies – Space Segment (3)
2. Engineering Focused Strategies – Ground Segment (2)
3. Engineering Focused Strategies – All Segments (2)
4. ConOps Focused Strategies (6)
5. Cyber Focused Strategies – Access (3)
6. Cyber Focused Strategies – System Design (3)
7. Cyber Focused Strategies – Software Design (1)

MRPP Interfaces

- Awareness
- Coordination
- Mitigations

DOD/IC Space agencies

Civil Space
NOAA, USGS

1 OCE-funded FTE

MRPP

MRPP Forum
(pending)

Mission Directorates

HEOMD SPO
(at JSC)

SMD

Lead for EP and Cybersecurity

established capabilities

GSFC

SAPP

JPL
Mission Protection

2 OCE-funded FTE

Centers

ARC

LaRC

MSFC

early efforts underway, mentored by MRPP

Agency Functions

Enterprise Protection
- Inter-/intra-agency coordination

OCIO
- Cybersecurity
- Supply chain

OIIR
- Intra-agency support and coordination

OPS
- Critical Infrastructure
- Intelligence

OSMA
- Supply chain
- Mission assurance

Forward Work

Near-Term

- (Re-)establish agency-wide forum to address MRPP-related topics
  Center participation and support is essential
- Improve sharing of threat-related information and associated mitigations
- Develop additional support materials to aid projects in implementing resilience and protection measures

Longer-Term

- Use MRPP forum to increase cadre of “protection-aware” personnel
- Address supply chain concerns, e.g., malicious functions in critical parts
  - Visibility into component-level and piece-parts usage
- Improve integration of cybersecurity into spaceflight systems
  - Train personnel, develop capabilities for improved cybersecurity resilience and robustness

Engineering Cybersecurity: Context

Impacts to NASA Missions From Malicious Actors [1]

Defense Intelligence Agency: With sophisticated knowledge of satellite [command and control] C2 and data distribution networks, actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems, associated ground infrastructure, users, and the links connecting them.

Defense Intelligence Agency (DIA); Report Number: DIA_F_01403_A;
Date of Publication: February 2019; Report Title: Challenges to Security in Space;
URL: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

Impacts to NASA Missions From Malicious Actors [2]

- NASA satellites have been contacted by unauthorized actors
- NASA engineering data has been copied without permission
- NASA mission operations have been interrupted by external actors

Defense Intelligence Agency: With sophisticated knowledge of satellite [command and control] C2 and data distribution networks, actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems, associated ground infrastructure, users, and the links connecting them.

Defense Intelligence Agency (DIA); Report Number: DIA_F_01403_A;
Date of Publication: February 2019; Report Title: Challenges to Security in Space;
URL: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

Impacts to NASA Missions From Malicious Actors [3]

- NASA satellites have been contacted by unauthorized actors
- NASA engineering data has been copied without permission
- NASA mission operations have been interrupted by external actors

Underlying issue: systems are not designed for cybersecurity outcomes

Defense Intelligence Agency: With sophisticated knowledge of satellite [command and control] C2 and data distribution networks, actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems, associated ground infrastructure, users, and the links connecting them.

Defense Intelligence Agency (DIA); Report Number: DIA_F_01403_A;
Date of Publication: February 2019; Report Title: Challenges to Security in Space;
URL: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

SPD-5: Space Policy Directive 5
Cybersecurity Principles for Space Systems (2020-09-04) [1]

Policy

Cybersecurity principles and practices that apply to terrestrial systems also apply to space systems. Certain principles and practices, however, are particularly important to space systems. For example, it is critical that cybersecurity measures, including the ability to perform updates and respond to incidents remotely, are integrated into the design of the space vehicle before launch, as most space vehicles in orbit cannot currently be physically accessed. For this reason, **integrating cybersecurity into all phases of development and ensuring full life-cycle cybersecurity are critical for space systems**. Effective cybersecurity practices arise out of cultures of prevention, active defense, risk management, and sharing best practices.

The United States must manage risks to the growth and prosperity of our commercial space economy. To do so and to strengthen national resilience, it is the policy of the United States that executive departments and agencies (agencies) will foster practices within Government space operations and across the commercial space industry that **protect space assets and their supporting infrastructure from cyber threats** and ensure continuity of operations.

The cybersecurity principles for space systems set forth in section 4 of this memorandum are established to guide and serve as the foundation for the United States Government approach to the cyber protection of space systems. Agencies are directed to work with the commercial space industry and other non-government space operators, consistent with these principles and with applicable law, to further define best practices, establish cybersecurity-informed norms, and promote improved cybersecurity behaviors throughout the Nation's industrial base for space systems.

https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

SPD-5: Space Policy Directive 5
Cybersecurity Principles for Space Systems (2020-09-04) [2]

Principles (summarized)

- Develop and operate space systems using **risk-based cybersecurity-informed engineering**
  - Continuously monitor, anticipate, and adapt to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations
  - Maintain an effective and resilient cyber survivability posture through the lifecycle
- Develop and implement **capabilities to maintain positive control**
  - Protect from unauthorized access (command, control, telemetry) using authentication or encryption
  - Physical protection to reduce vulnerabilities of space command, control and telemetry receivers
  - Protection against jamming and spoofing
  - Protection of ground systems
  - Cybersecurity hygiene practices
  - Manage supply chain risk
- Implement rules and guidance to enhance space system cybersecurity, including best practices and norms of behavior
- Collaborate to develop best practices, including sharing of threat, warning, and incident information within the space industry
- **Design security measures to be effective while managing risk tolerances and minimizing undue burden**

https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

NASA Cybersecurity Task Team (CTT)

From the Executive Summary (July 2020):

- The Cybersecurity Task Team was chartered in March 2019 by the Enterprise Protection Board to benchmark the policies and implementation approach to cybersecurity for robotic space flight and ground systems used by other organizations, evaluate existing NASA policies and procedures, and propose updates to, or additional content for, these policies and procedures. The ultimate goal is to strengthen robotic space flight and ground system cybersecurity in a manner that is implementable and achievable by space flight projects and programs. This team was to include center expertise in space flight system development and operations, space flight system protection, and cybersecurity policy.

Recommendations across four topics:

- Staffing
- Risk Management
- Development
- Information Sharing

CTT met with and benchmarked multiple external organizations to gain a broad perspective regarding potential best practices to adopt at NASA

NASA CTT Final report (July 2020)
Selected Recommendations

- S-1: Ensure a mission cybersecurity engineer is assigned to the system engineering team.
- S-2: Provide cybersecurity training for all project discipline engineers so the cybersecurity impacts to all systems are considered from the outset.
- S-3: Budget for cybersecurity from the beginning (and throughout the lifecycle).
- RM-1: Ensure cybersecurity risks are considered as part of the risk management process.
- RM-7: Ensure a risk-based decision process is used to determine whether to mitigate an identified vulnerability.
- D-4: Ensure design decisions are assessed with an understanding of the cybersecurity threat environment and risks associated with that decision.
- D-8: Design systems to have a safe mode Conops during an attack and resilience to recover from cyber attacks.
- D-9: Ensure cybersecurity aspects are included in project incident response plans.
- D-10: Ensure systems are designed to be patched or upgraded throughout the lifetime of the mission, and allow for continuous monitoring, without major impact to operations.
- D-14: Utilize penetration testing as a method to validate the effectiveness of the implementation with respect to security.

Engineering Cybersecurity

Need to Evolve

We need to evolve our engineering practices to encompass cybersecurity outcomes

- ”Build security in, don’t bolt it on” / “Baked-in security”
- Avoid or contain system vulnerabilities to known or postulated threats

Cybersecurity is a set of emergent properties of the system’s design and use – better designs yield better results

- Various capabilities can amplify or disrupt these properties
- Trade space needs to be considered during the engineering processes
- Cross-discipline expertise is needed to identify and manage these properties
- Not sufficient to address this at the project/mission level – necessary, not sufficient

System engineering is the logical focus area – enables a system-wide perspective that maintains focus on successful system delivery

Systems Security Engineering

Systems security engineering as a specialty / sub-discipline of systems engineering

- Build on existing engineering disciplines and capabilities, including engineered tolerance and resilience
- Reduce or control the effects of disruptions, hazards, and threats
- Implies predictability of and transparency in the system to identify, prevent, react, adapt, or recover from anomalous elements (helps reduce complex to complicated)

Goal: Systems that are less susceptible to the effects of an intelligent adversary*

* “effects of an intelligent adversary” does not always require intelligence or adversaries

Other engineering disciplines need to consider cybersecurity as an explicit element, can be coordinated from the systems security

- Software is often the easiest engineering area in which to reason (inc. firmware, FPGA) – applies to any logic paths such as in hardware (e.g., circuits, mechanical triggers)

Examples of Cybersecurity in SE Processes

System Design Processes

- Stakeholder Expectations: Federal and NASA guidance on protecting systems with cybersecurity measures
- Technical Requirements Definition: Some cybersecurity controls are constraints (e.g., NASA network operating environment), others inform trade space (e.g., integrity controls)

Technical Management Processes

- Interface Management: Establish cybersecurity expectations and objectives
- Technical Risk Management: Incorporate cybersecurity context into risk considerations, particularly those from a malicious source and intent
- Configuration Management: Traceability of cybersecurity outcomes

Product Realization Processes

- Product Integration: Use existing infrastructure (e.g., NASA network, cybersecurity monitoring)
- Product Verification: compliance with system security plans (Authorizations to Operate)
- Product Validation: end-to-end testing includes adversarial cybersecurity testing techniques (penetration testing)

Examples of Cybersecurity in Software Processes

Existing Software Requirements in NPR 7150.2C:

- Perform a system-based software cybersecurity assessment on the software components per the Agency security policies and the project requirements, including risks posed by the use of COTS, GOTS, MOTS, OSS, or reused software components
- Identify cybersecurity risks, along with their mitigations, in flight and ground software systems and plan the mitigations for these systems.
- Implement protections for software systems with communications capabilities against unauthorized access
- Ensure that space flight software systems are assessed for possible cybersecurity vulnerabilities and weaknesses
- Address identified cybersecurity vulnerabilities and weaknesses
- Test the software and record test results for the required software cybersecurity mitigation implementations identified from the security vulnerabilities and security weaknesses analysis
- Identify, record, and implement secure coding practices
- Verify that the software code meets the project's secure coding standard by using the results from static analysis tool(s)

Examples of Cybersecurity Concerns

Critical cybersecurity issues can derive from:

- Allowing too many privileges to a person or function
- Allowing too much access / too many interfaces
- Defects, e.g., implementation bugs such as buffer overflows and design flaws
- Inconsistent error handling
- Lack of operational data to find cybersecurity issues
- Failing to properly manage memory allocations / use
- Failing to validate data or requests
- Discrepancies in logical interfaces (usually due to assumptions, insufficient precision)
- Changing from “as designed” to “as operated”
  - Ex. legacy operating system or software support
- Over-dependence on system-external services / functions
- …

System Security Engineering Support at the Project Level

Project-level system security engineering:

- Projects should have dedicated staff time for this area, larger projects may need to dedicate multiple individuals
- Chief Information Security Officer (CISO) subject-matter experts can provide insight and advice
- Is not sufficient to define this as the Information System Security Officer (ISSO) role defined by NIST

Sample responsibilities:

- Serve as native translator between the project, engineering, assurance, and CISO teams
  - If not the expert, knows where to find one
- Champion for all cybersecurity causes within the project team – as balanced with sound system design and risk management
- Manage cybersecurity requirements and constraints to be implemented within the project constraints
- Support feasibility studies and trade analysis with cybersecurity context – how are cybersecurity outcomes improved/affected by the effort? What cybersecurity-enabling features are being considered?
- Monitor the full system's environment "end-to-end" for potential new cybersecurity concerns
  - Needs visibility into systems the project depends upon, and does not directly operate (e.g., communications networks, flight dynamics)
  - Considers impacts from changes in the external environment of the system (e.g., communications networks, malicious attack trends)
- Cogently present cybersecurity topics within the review processes
- Document "cybersecurity manual" for the system, so that future users understand how "as designed" may need to be changed "as operated"
  - Identify operational needs of a future system to take advantage of the cybersecurity capabilities built into the system
- Develop cybersecurity protection and incident response plans
  - During Implementation Phase, protecting critical data and functions
  - During Operations Phase, support system to mitigate emergent vulnerabilities, support CISO cybersecurity incident response

Addressing Risks

Projects are accountable for cybersecurity outcomes

- Responsible for ensuring cybersecurity is addressed in all facets of the project
- Commonly need to make use of project-external service providers
- Manage risks that may include cybersecurity aspects

Systems security engineer responsible for identifying and monitoring risks with cybersecurity aspects, and to help identify cybersecurity-related trade space across the system

- Working within the project team to ensure cybersecurity concerns are recognized
- Working with external providers to coordinate cybersecurity concerns
- Consulting with CISO teams for subject-matter expertise

Independent reviews should include cybersecurity considerations in all areas where risk is addressed

Share risk context and decisions with other teams to improve overall risk management

Technical Authority

No change to technical authorities (TA)

For issues requiring TA, that involve cybersecurity, TA should include OCIO inputs to the discussion – decision remains with TA

- Ex., Center TA would engage with Center CISO for insight and context

Suggested Actions

[Center] Engineering and Assurance teams:

1. Assess existing engineering and assurance capabilities to address cybersecurity concerns, develop gap analysis
2. Incorporate features to support or enhance cybersecurity concerns in ongoing engineering and assurance efforts, including system design, software, architecture plans
3. For projects, ensure responsibility for engineering and assurance cybersecurity is identified, appropriate to the scope of the project and lifecycle phase
4. Incorporate cybersecurity concerns into risk considerations
5. Address cybersecurity topics as part of independent reviews
   - Not solely for compliance with OCIO policies – necessary, not sufficient
6. Ensure contracts supporting engineering include cybersecurity concerns in contractual requirements and work products
7. Report implementation status, suggestions, and concerns to OCE in ~May 2021.

This is a living effort that will evolve over time with your support.

Forward Work

Develop training resources tailored for engineering professionals

- "*Essential cybersecurity for engineering professionals*" is, surprisingly, not a common course offering
- Similarly "*Essential engineering for cybersecurity professionals*" is also not a common course offering

Develop sample documents and guides, such as:

- System engineering management plan elements for cybersecurity
- Safety and Mission Assurance plan for cybersecurity assurance elements
- Whitepapers

Continue working with OCIO and OSMA to improve communications and tailoring / risk acceptance options

Improve commonality of risk decisions across multiple projects and organizations

- Legacy systems, "high risk" missions (e.g., Class D), when to mitigate (and at what level)

Time for Discussion, Q&A

Backup Content

NASA Protection Guidance, Summary

NASA Enterprise Protection Guidance

- NPR 1058.1, June 2019, NASA Enterprise Protection
  - Establishes the roles and responsibilities related to the Principal Advisor for Enterprise Protection, the Enterprise Protection Program (EPP), and the Enterprise Protection Board (EPB)
- NID 1058.127, May 2020
  - Mandates use of STD-1006 for all programs and projects started after February 2019
  - Succeeds AA memo from February 2019

NASA Space Protection Guidance

- NPR 7120.5, August 2012, NASA Space Flight Program and Project Management Requirements
  - Requires a project protection plan based off threat summaries
- NPR 7120.8, September 2018, NASA Research and Technology Program and Project Management Requirements
  - Requires a protection plan for projects operating in space
- Candidate Protection Strategies
  - Starting point for developing a protection plan, series of questions related to best practices to mitigate high threat and risk issues
- NASA-STD-1006: Space System Protection Standard
  - Baseline standards to improve space system protection from well understood threats

Note also: related guidance for physical/industrial security (NPD 1600 series), and information security (NPD 2810 series)

NASA Engineering Network (NEN) Mission Resilience and Protection Community of Practice site:

- https://nen.nasa.gov/web/sap

What is Enterprise Protection? Overview

Office of the Administrator

Threat Intelligence

Indications and Warning
NSDC, CSpOC

System Protection and Technical Coordination
e.g., SSDP, NRO, SF, NOAA, USGS

Principal Advisor for Enterprise Protection (PAEP)

Per EP NPR, organizations with lead authority and responsibility for protection of systems under their cognizance:

☆ Mission Directorates
ARMD, HEOMD, SMD, STMD

☆ HQ Functional Offices
e.g., OCE, OCIO, OSI

☆ Centers
AFRC, ARC, GRC, GSFC, JPL, JSC, KSC, LaRC, MSFC, SSC

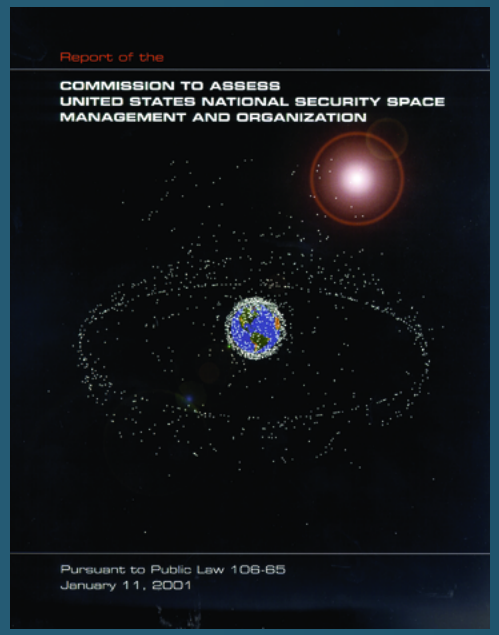
☆ = Enterprise Protection Program personnel (federated)

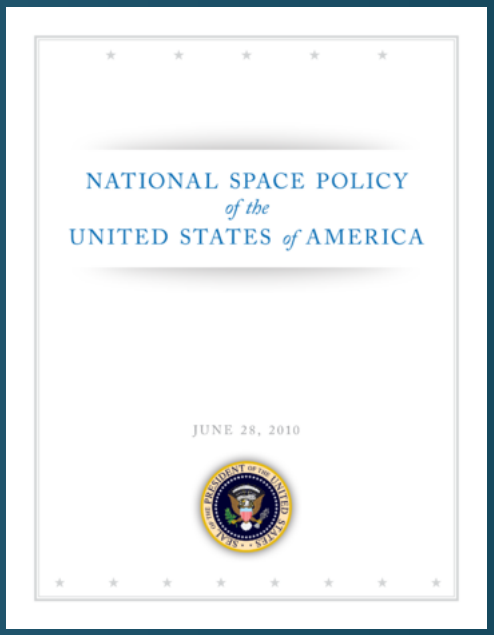
Agency Strategic Objective 4.5: Ensure Enterprise Protection

"Increase the resiliency of NASA's enterprise systems by assessing risk and implementing comprehensive, economical, and actionable solutions."

NPR 1058.1 NASA Enterprise Protection Program

Key National Documents





2001-01-11: **Commission to Assess US National Security Space Management and Organization** aka "Rumsfeld Commission"

- Space systems are vulnerable
- US is dependent on space
- Focuses mostly on DOD and the Intelligence Community
- Served as a call to action to clarify US goals in space

2010-06-28: **National Space Policy of the United States of America**

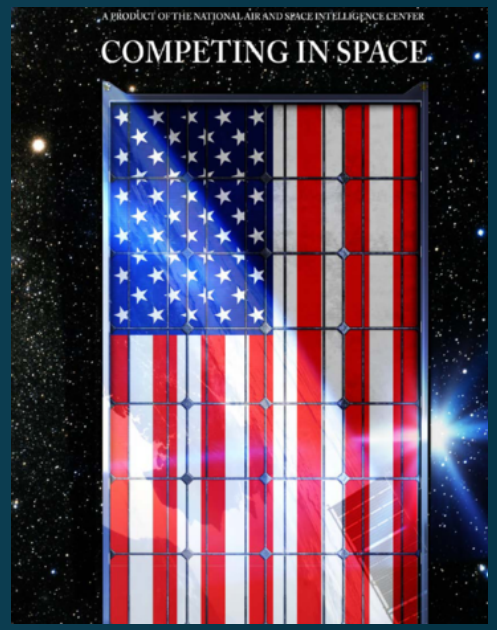
- Establishes US principles for space, including peaceful exploration, responsible actions
- US goals include cooperation, assurance and resilience, and Earth and solar observation

Amended in 2017 to expand NASA's exploration goals to include Moon and Mars.

2011-01: **National Security Space Strategy** (Unclassified Summary)

- Space is congested, contested, and competitive
- Improve space situational awareness and transparency
- Deter aggression in space
- Strengthen resilience

Newer documents have since been issued.

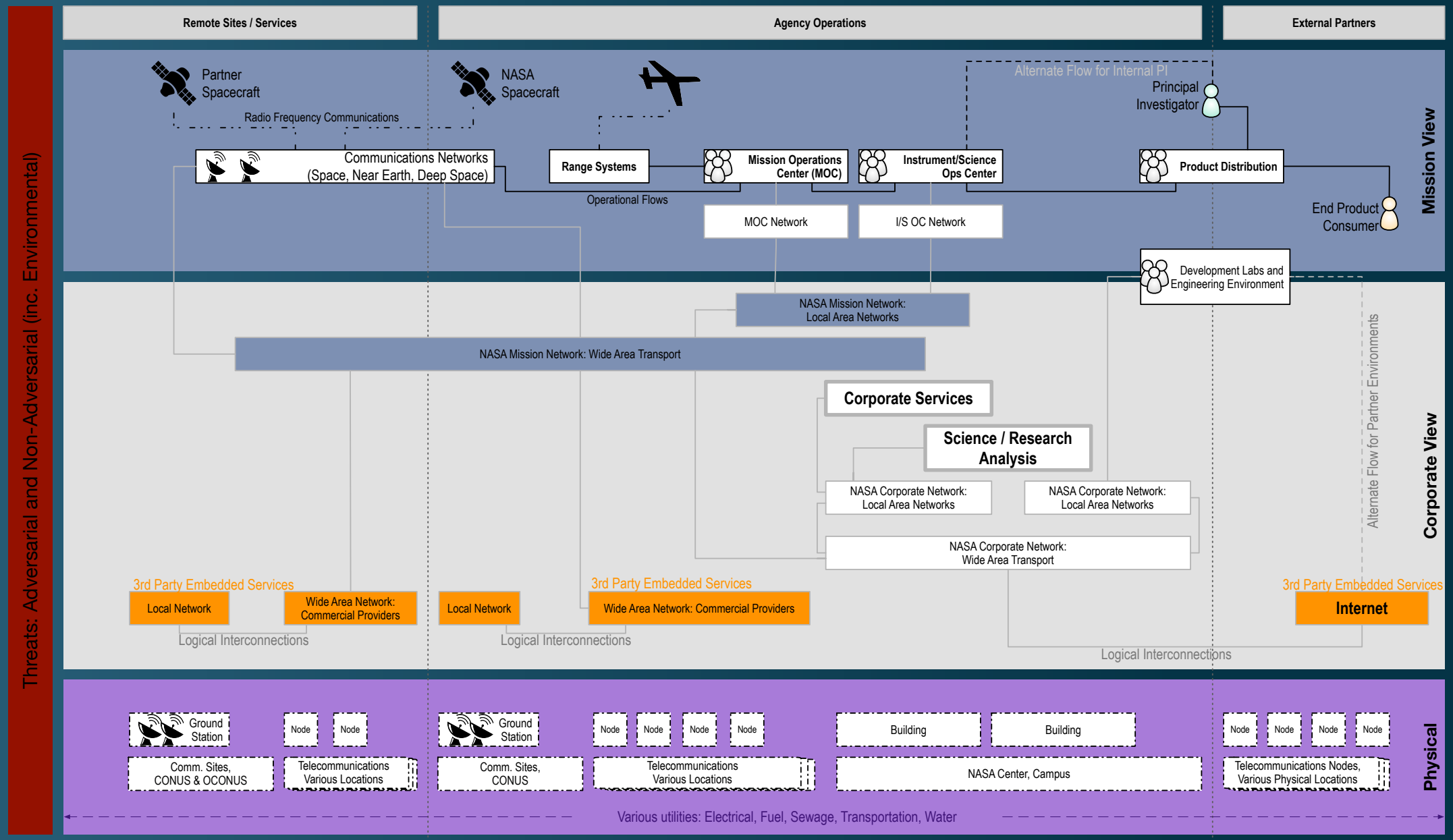


2018-12: **NASIC: Competing in Space**
2019-02: **DIA: Challenges to Security in Space**

- First public US documents describing specific counterspace threats associated with individual countries
- Overview of types of capabilities and potential effects on space systems and their support systems
- Details about counterspace capabilities available to other nations, and the perceived motivations for use

Notional View of Security Layers (with Representational Elements)

2017-07-03 rev1

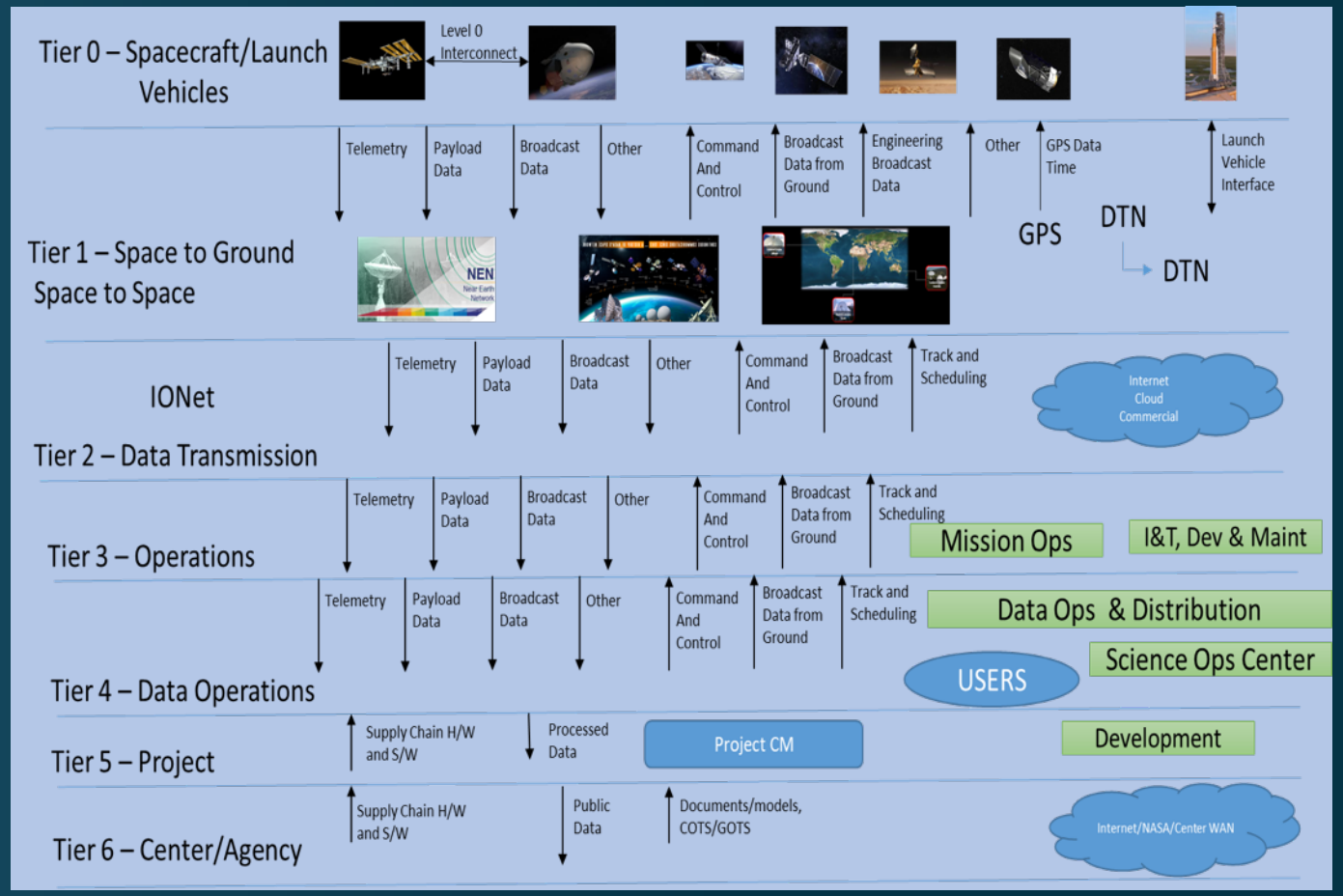


Enterprise Protection
Complexity of Mission Systems

Unique Challenge of Mission System Vulnerability Assessments and Risk Mitigation

Mission systems, especially space segment and ground-space communications systems, are:

- Significantly more complex than corporate IT systems (multiple Tiers),
- Often have legacy hardware (e.g. RAD750) that was designed decades ago without security in mind,
- Often have legacy software that were never designed with security in mind,
- Often have legacy architectures, protocols, data interchange formats, and commanding formats that were never designed for security.
  - Analogous to the Internet not being designed with today's security needs in mind:
    - *"We didn't focus on how you could wreck this system intentionally," said Vinton G. Cerf*

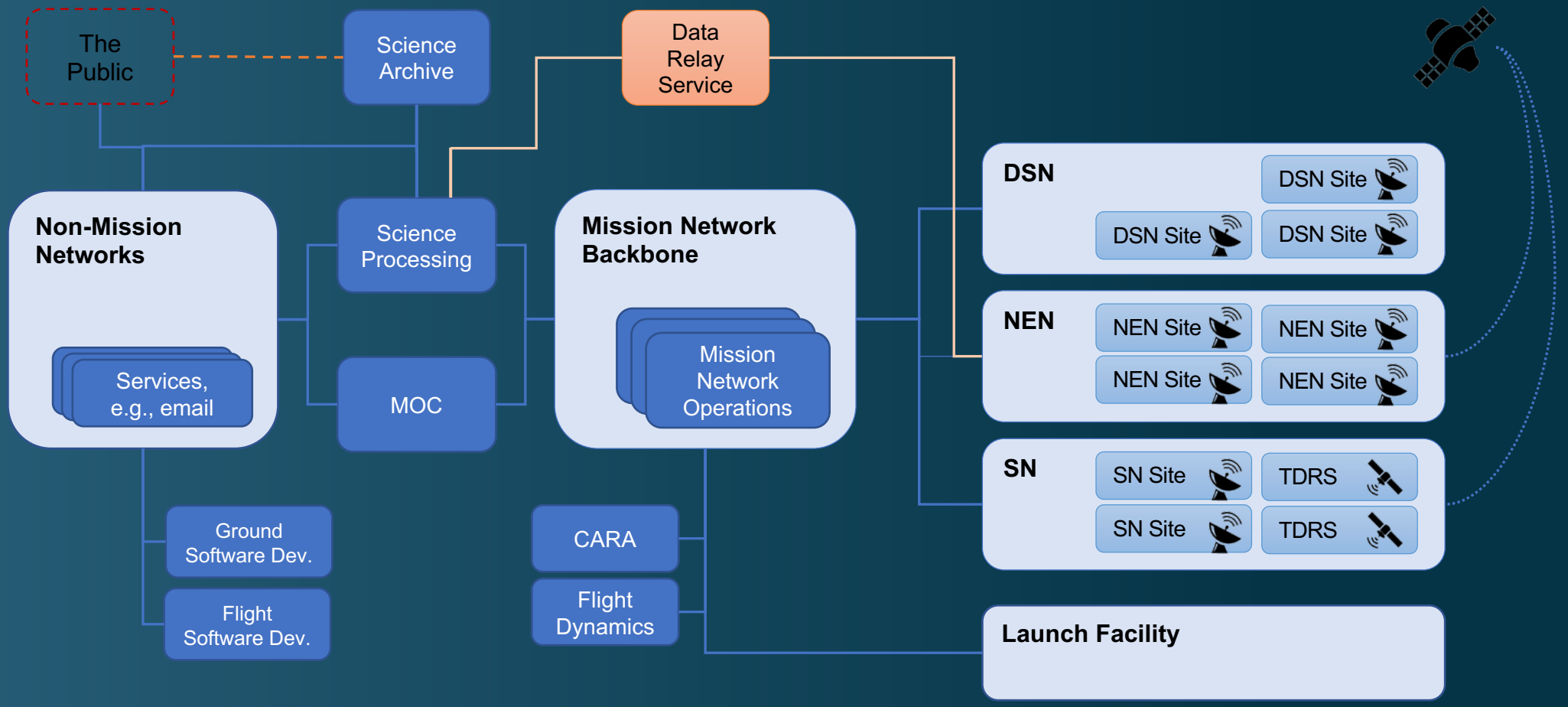


Current processes are not sufficient to discover vulnerabilities

Credit: IV&V Mission Protection Services Group

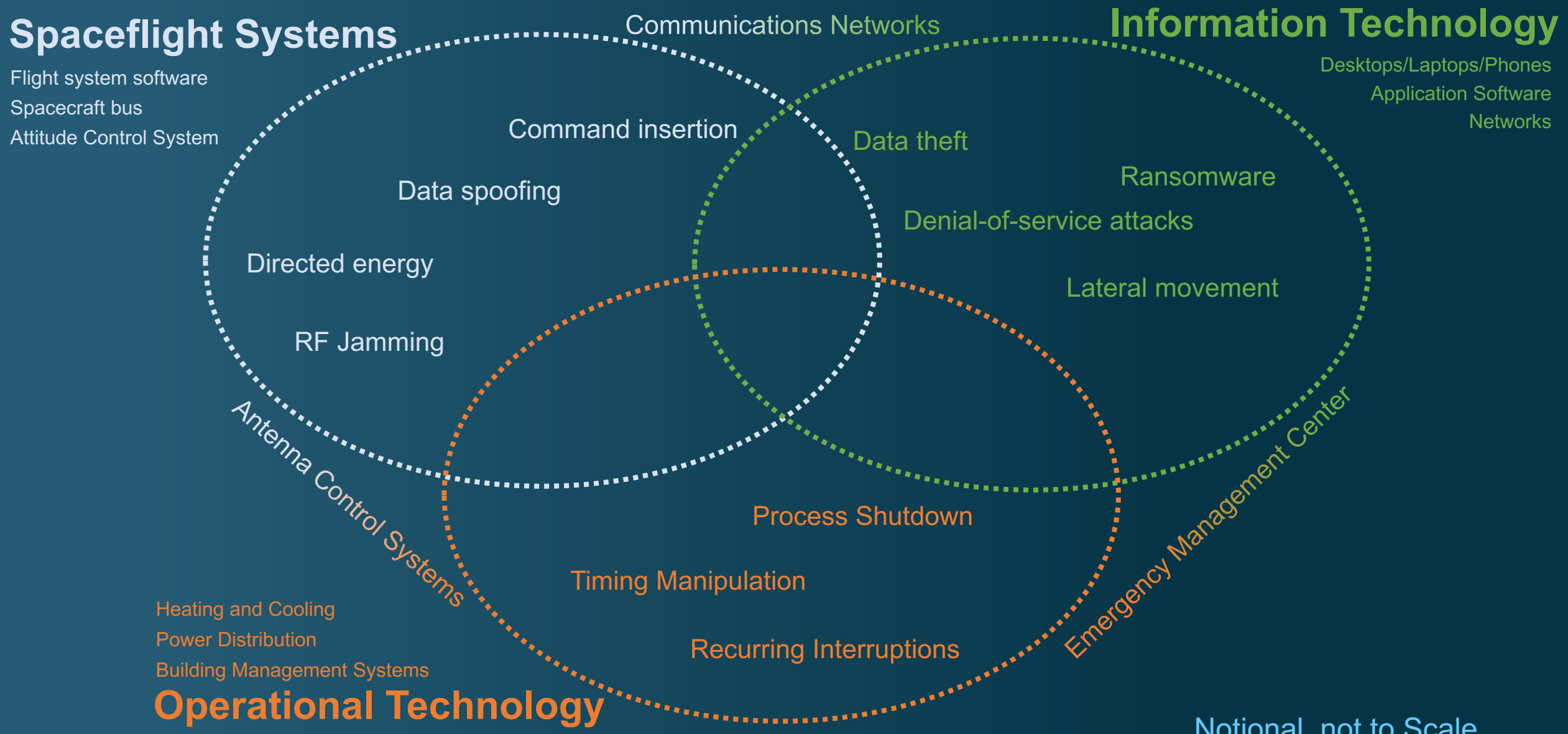
Mission Network / SSP Model

Notional GSFC Science Mission



- Each shaded box represents a system security plan or sub-plan boundary
- The actual (technical and organizational) interfaces are somewhat more complex

Many Perspectives on Cybersecurity and “Threats”



Notional, not to Scale

Hackasat: Space Security Challenge 2020

- Sponsored by USAF and AFRL, overall goal to build safe, reliable, and trustworthy operations (by studying weaknesses and fixing them)
  - Qualification round May 2020 with 1,278 teams
- Sample challenges included:
  - Calculate attitude quaternion from boresight reference vectors
  - Identify and exploit bug in an attitude control algorithm
  - Extract memory contents across I2C bus
  - From MIPS or SPARC firmware images, exploit a weakness

https://hackasat.com
https://github.com/deptofdefense/hack-a-sat-library

NIST SP 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (draft, August 2017)

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigate cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

MITRE Common Weakness Enumeration (CWE)

Three Views (Software Development, Hardware Design, Research Concepts)

699 - Software Development

- API / Function Errors - *(1228)*
- Audit / Logging Errors - *(1210)*
- Authentication Errors - *(1211)*
- Authorization Errors - *(1212)*
- Bad Coding Practices - *(1006)*
- Behavioral Problems - *(438)*
- Business Logic Errors - *(840)*
- Communication Channel Errors - *(417)*
- Complexity Issues - *(1226)*
- Concurrency Issues - *(557)*
- Credentials Management Errors - *(255)*
- Cryptographic Issues - *(310)*
- Data Integrity Issues - *(1214)*
- Data Processing Errors - *(19)*
- Data Neutralization Issues - *(137)*
- Documentation Issues - *(1225)*
- File Handling Issues - *(1219)*
- Encapsulation Issues - *(1227)*
- Error Conditions, Return Values, Status Codes - *(389)*
- Expression Issues - *(569)*
- Handler Errors - *(429)*
- Information Management Errors - *(199)*
- Initialization and Cleanup Errors - *(452)*
- Data Validation Issues - *(1215)*
- Lockout Mechanism Errors - *(1216)*
- Memory Buffer Errors - *(1218)*
- Numeric Errors - *(189)*
- Permission Issues - *(275)*
- Pointer Issues - *(465)*
- Privilege Issues - *(265)*
- Random Number Issues - *(1213)*
- Resource Locking Problems - *(411)*
- Resource Management Errors - *(399)*
- Signal Errors - *(387)*
- State Issues - *(371)*
- String Errors - *(133)*
- Type Errors - *(136)*
- User Interface Security Issues - *(355)*
- User Session Errors - *(1217)*

1194 - Hardware Design

- Manufacturing and Life Cycle Management Concerns - *(1195)*
- Security Flow Issues - *(1196)*
- Integration Issues - *(1197)*
- Privilege Separation and Access Control Issues - *(1198)*
- General Circuit and Logic Design Concerns - *(1199)*
- Core and Compute Issues - *(1201)*
- Memory and Storage Issues - *(1202)*
- Peripherals, On-chip Fabric, and Interface/IO Problems - *(1203)*
- Security Primitives and Cryptography Issues - *(1205)*
- Power, Clock, and Reset Concerns - *(1206)*
- Debug and Test Problems - *(1207)*
- Cross-Cutting Problems - *(1208)*

1000 - Research Concepts

- Improper Access Control - *(284)*
- Improper Interaction Between Multiple Correctly-Behaving Entities - *(435)*
- Improper Control of a Resource Through its Lifetime - *(664)*
- Incorrect Calculation - *(682)*
- Insufficient Control Flow Management - *(691)*
- Protection Mechanism Failure - *(693)*
- Incorrect Comparison - *(697)*
- Improper Check or Handling of Exceptional Conditions - *(703)*
- Improper Neutralization - *(707)*
- Improper Adherence to Coding Standards - *(710)*

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

v4.1 (June 2020) lists 875 weaknesses

https://cwe.mitre.org