AEROSPACE REPORT NO.
TOR-2021-01333-REV A

Cybersecurity Protections for Spacecraft: A Threat Based Approach

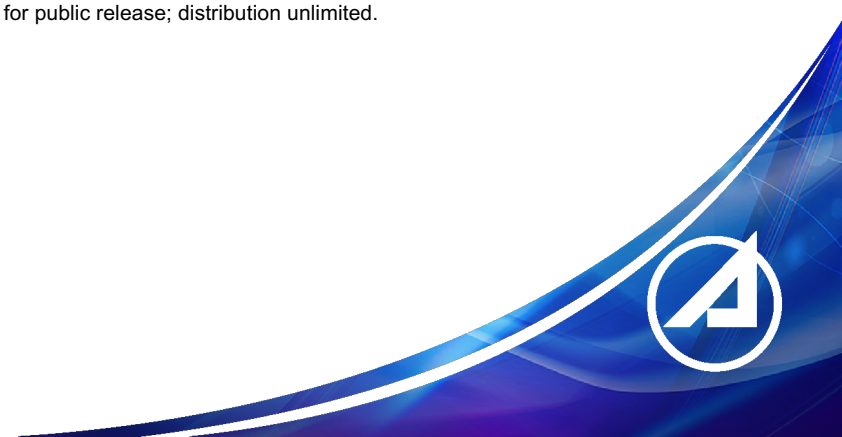
April 29, 2021

Brandon Bailey
Cyber Assessment and Research Department (CARD)
Cybersecurity Subdivision (CSS)

Prepared for:
U.S. GOVERNMENT AGENCY

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group



Abstract

Space systems are leveraged by many government and commercial entities to provide global capabilities unique to the space domain. During a conflict, adversaries will seek to disrupt, deny, degrade, deceive, or destroy those capabilities. Cyberattacks are a complex but effective and increasingly prevalent attack vector in the space domain. To counter the threat posed by cyberattack, cybersecurity and space operations are becoming inextricably linked.

Historically, spacecraft had been considered relatively safe from cyber threats and space system vulnerabilities were often overlooked in evaluation of critical infrastructure. With space cyber threats emerging from nation-state actors, government and industry stakeholders identified that additional defenses should be implemented. Space-centric cybersecurity standards and governance have been slow to materialize, however, and are lagging behind the growth of the cyber threat. Defense-in-depth techniques for space system protection must be adopted across the government, industry, and international community to ensure space systems are resilient to cyber compromise. Potential solutions will include increased cooperation across these domains and require a blend of policy, standards, and technical solutions.

One thrust of this collaborative effort is a threat-informed risk mitigation strategy to protect space systems. This analysis describes the background of space system cybersecurity and the state of existing standards, the concepts of defense-in-depth protection necessary to protect spacecraft, and then a threat-oriented approach to space cyber risk assessment. The ultimate result of this analysis is a set of products that define risk driven requirements to utilize during acquisition and operations for better space system protection.

Contents

Figures

Tables

1 Introduction

"The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. Therefore, it is essential to protect space systems from cyber incidents in order to prevent disruptions to their ability to provide reliable and efficient contributions to the operations of the Nation's critical infrastructure." – Space Policy Directive 5 (SPD-5) [1]

SPD-5 was released by the President on September 4, 2020 as "Cybersecurity Principles for Space Systems" and baselined many aspects advocated within the space community to protect systems. SPD-5 defines a "space system" as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service." Space systems comprise many government and commercial components where cybersecurity and space operations are inextricably linked. The threats to ground infrastructure and spacecraft are often overlooked in wider discussions of cyber threats to critical national infrastructure. With the emergent cyber threats to space systems from nation-state actors, there is a need to bolster space system defenses with more security principles.

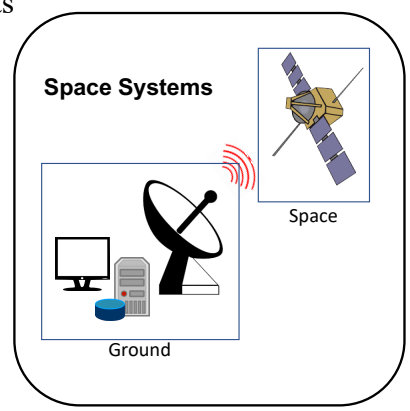


Figure 1: Space Systems

Historically, spacecraft have been considered relatively safe from cyber intrusions; however, recent activity has shown that the spacecraft themselves are in the sights of our adversaries. While space centric cybersecurity standards and governance continue to lag behind, adoption of defense-in-depth techniques for space systems will help ensure space systems are resilient to cyber intrusion. The push towards a comprehensive cyber defense strategy will require a blend of policy, governance/oversight, and technical solutions. As one of the first thrusts towards modernizing space cyber defenses, a threat informed risk mitigation strategy should be used to quickly focus resources on protecting the assets that perform or contribute to our nation's critical capabilities.

With the western world's growing dependence on space systems to support commercial markets and government capabilities, nation states have developed capabilities targeting those systems. As depicted in Figure 2, there are many threats to space systems. [2]

"There is a clear trend toward lower barriers to access, and widespread vulnerabilities coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and will likely grow in severity over the next decade, there remains a stark difference at present between the cyberattacks capabilities of leading nation-states and other actors." – Global Counterspace Capabilities: An Open Source Assessment [3]

This paper focuses on cyber threats due to several factors that make the attack vector attractive to an adversary. Some space systems utilize a single ground system to operate multiple spacecrafts or multiple missions. An

attack on this type of ground system threatens to impact multiple targets with a single compromise. In addition, cyberattacks with good operational security (OPSEC) and countermeasures make source attribution difficult and would delay any coordinated response. Cyberattacks are accomplished through computer systems that operate at very fast timescales. These short timeframes can significantly reduce defensive reaction time and provides significant advantage for threat actions to be accomplished without response. Lastly, cyberattacks have been shown to yield limited response in the form of military or economic conflict escalation or retaliatory responses [4], making cyberattack a more palatable alternative than other acts of aggression.

Compared to other classes of anti-satellite weapons [2], cyber weapons are generally significantly cheaper and can be developed on shorter timeframes as there is no physical manufacturing required. Software-based cyber weapons provide the adversary significant flexibility in their choice of effects to have on the space system - including actions that are reversible or irreversible. Cyberattacks can destroy satellites without creating debris for less collateral damage or even simply take over the platform. The high-radiation space environment makes system failures more common on spacecrafts, and without the physical access we have on ground systems, consequently, makes outage attribution much more challenging.

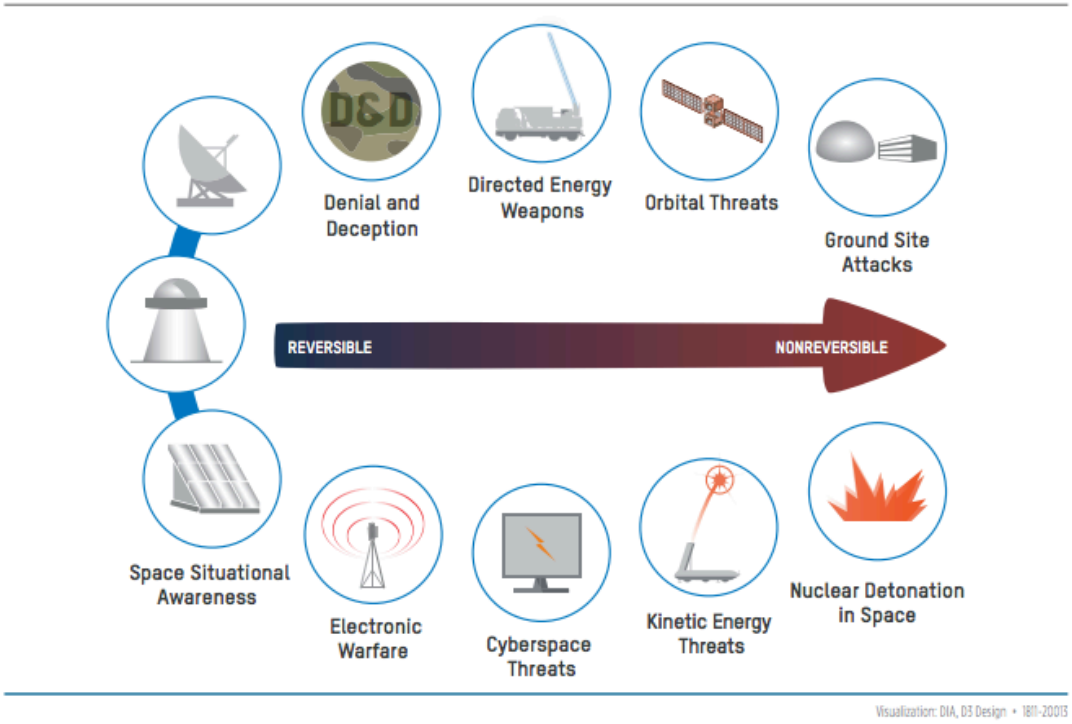


Figure 2: Counterspace Continuum for Attacks [2]

Cyberattacks can be used to affect the confidentiality or integrity of the information gathered or produced by the space system. A compromise of this information would reduce the confidence or even the usefulness of the space system. Cyberattacks can also be used to affect the availability of the space systems such that critical capabilities are not there when needed. An example of an

availability attack would be temporarily affecting the space system's ability to provide communications or collect information in times of critical need. Irreversible effects might also be achievable, such as: firing thrusters, emptying propellant, destabilizing the orbit, causing the satellite to re-enter the atmosphere, locking up the on-board computer for ransom, depleting the power sources, or even pointing optical sensors towards the sun to damage the focal plane.

As vulnerability research and open-source intelligence on space systems increases, attacks exploiting these existing vulnerabilities will likely increase. In recent years, researchers have published proof of concepts attacking satellite communication and the Iridium satellite network. [5], [6]. Presentations at BlackHat USA 2020 [7] and the evolution of the Aerospace Village at DEFCON is an indication that space system security awareness is growing. Maturing attack vectors will increase risk across the space domain whether the asset owner is military, government, commercial, or scientific.

1.1 Scope and Purpose

This document is intended to provide guidance and requirements for developing more secure space systems, but particularly with a focus on the spacecraft. The scope can be articulated using these key questions:

- **Who:** Anyone developing a spacecraft (e.g., commercial, government, university).
- **What:** Threat informed, risk-based cybersecurity requirements.
- **When:** During the early phases of system development. These needs also span development through operations and sustainment.
- **Why:** Threat landscape has evolved, and spacecraft are being targeted by adversaries using cyber means.
- **How:** Ranking cyber threats against the space system design to determine highest risk areas and then adding cybersecurity requirements to reduce cyber risk.

While many of the following security principles are linked and informed by United States government security documents, these principles apply to any space system and should be implemented accordingly to reduce cyber risk to a defined risk tolerance.

1.2 Existing Cybersecurity Standards

The U.S. federal governance structure for general information technology (IT)-based cybersecurity has made strides in recent years with the maturation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and Cybersecurity Framework (CSF). However, parallel progress specific to the space domain has not been made. NIST cybersecurity maturity standards and guidelines help organizations to improve their cybersecurity measures and best practices, but these aspects are not all directly applicable to the space domain. For example, taking the default NIST SP 800-53 moderate impact baseline for a system, around 75% of controls are not applicable to a typical spacecraft. In addition, there are around 80 security controls from the NIST control list that should apply, but they are not "default" in the pre-established low-moderate-high impact baselines. While efforts have been made to mold these frameworks for space systems (e.g., Committee on National Security Systems [CNSS] Instruction [CNSSI] 1253F), uniformity is lacking, and updated standards and guidelines for space systems are likely warranted.

SPD-5 identified this gap and has established 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." SPD-5 goes on to say, "implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity, including through the consideration and adoption, where appropriate, of cybersecurity best practices and norms of behavior."

While there are no approved space cybersecurity standards that are widely adopted, there are pockets of initiatives across the space community that are addressing cybersecurity for space systems. Table 1 outlines some of the known initiatives and standards that have been published relating to cybersecurity within the space domain. Limited published work is available for reference; however, the papers *Cyber Enhanced Space Operations* and *Defending Spacecraft in the Cyber Domain* recommend several strategies for more secure space systems and operations. [8], [9] Other nonpublished initiatives are underway within the federal government, but at this point all these initiatives are too early to reference as adopted practices and mostly focus on the ground segment. The published security standards listed in the table range from high-level compliance controls to low-level communication protocol standards and are not overarching engineering principles for space systems which is the focus of this paper.

Table 1. Known Cybersecurity Initiatives and Standards

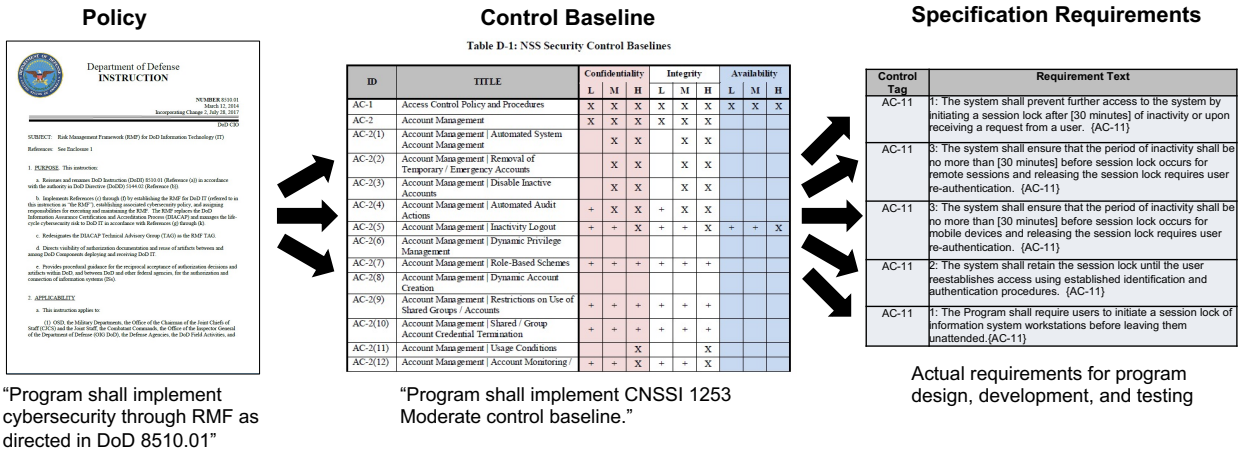
Organization	Title of Standard	Applicability / Scope	Link to Standard	Description of Standard
CNSS	CNSSI 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions	Ground & Spacecraft for National Security System (NSS) only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	Elaborates how to appropriately integrate Information Assurance into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems.
CNSS	CNSSI 1253F Attachment 2 Space Platform Overlay	Unmanned spacecraft for NSS only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	Applies to the space platform portion of all space systems that must comply with CNSS Policy No. 12. The controls specified in this overlay are intended to apply to the space platform after it is launched and undergoing pre-operational testing and during operation. This overlay attempts to mold NIST SP 800-53 for the space segment.
Consultative Committee for Space Data Systems (CCSDS)	352.0-B Cryptographic Algorithms	Civilian Space Communications	https://public.ccsds.org/Pubs/352x0b2.pdf	Provides several alternative authentication/integrity algorithms which may be chosen for use by individual missions depending on their specific mission environments. Does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis.
Consultative Committee for Space Data Systems	355.0-B Space Data Link Security (SDLS) Protocol	Civilian Space Communications	https://public.ccsds.org/Pubs/355x0b1.pdf	This protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and

Organization	Title of Standard	Applicability / Scope	Link to Standard	Description of Standard
				Advanced Orbiting Systems Space Data Link Protocols to provide a structured method for applying data authentication and/or data confidentiality at the Data Link Layer.
Consultative Committee for Space Data Systems	356.0-B Network Layer Security	Civilian Space Communications	https://public.ccsds.org/Pubs/356xb1.pdf	Provides the basis for Network Layer security for space missions utilizing the Internet Protocol (IP) and complying with IP over CCSDS Space Links
Consultative Committee for Space Data Systems	357.0-B Authentication Credentials	Civilian Space Communications	https://public.ccsds.org/Pubs/357x0b1.pdf	CCSDS credentials are needed to allow authentication between communicating entities for authorization and access control actions. CCSDS recommends two types of credentials in this standard: X.509 certificates and protected simple authentication.
Aerospace Industries Association	NAS9933 Critical Security Controls for Effective Capability in Cyber Defense	Department of Defense (DOD) Aerospace Contractors Enterprise/Ground Infrastructure	http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf	To align the fragmented and conflicting requirements that the DOD contracting process imposes on industry. Rather than different DOD organizations using different tools to assess a company's security across different contracts, this standard is designed to apply common and universal elements of cybersecurity across each enterprise.
NASA	Space System Protection Standard	Applicable to all NASA programs and projects (starting in 2020)	https://standards.nasa.gov/sites/default/files/standards/NASA/PUBLISHED/Baseline/nasa-std-1006.pdf	Establishes Agency-level protection requirements to ensure NASA missions are resilient to threats and is applicable to all NASA programs and projects starting in 2020.

To demonstrate inconsistency in cybersecurity standard protection, an example comparison can be performed between the two primary government space systems publications: CNSSI 1253 for National Security Systems (NSS) and NIST Special Publication (SP) 800-53 for U.S. civil space systems. While CNSSI was created as an enhancement to NIST SP 800-53, there are notable differences in the resulting requirements derived from the standards. For a moderate impact categorization level, the CNSSI 1253 baseline requires approximately 389 controls compared to 262 required for the NIST SP 800-53 baseline. As a baseline comparison, NSS requires an additional 127 security controls above those defined for a civil space system. Many of the enhanced controls reside within the Access Control (AC), Identification and Authentication (IA), and System and Communications Protection Control (SC) families, which are extremely important for any system to prevent adversaries from accessing the space system. This basic analysis shows that civil systems will by default be analyzing and implementing fewer basic protections and therefore be more vulnerable. This is problematic as space threats are continuing to evolve and will likely target U.S. military and civilian space systems during conflict.

Aerospace evaluations show a specific example of improper control tailoring of NIST SP 800-53 revision 4 controls IA-2(8) and IA-2(9) being scoped out of spacecraft control baselines as being not applicable. These two controls state "The information system implements replay-resistant authentication mechanisms …". Within space system context, radio frequency replay attacks are one of the largest threat vectors to the spacecraft and should always be mitigated with control countermeasures. Additional countermeasures such as wireless communication protection, on-board monitoring/logging, and software integrity are also incorrectly scoped out from many spacecraft baselines.

Many government backed spacecraft development initiatives usually follow a flow similar to Figure 3 below. A policy document (e.g., DODI 8510.01, NASA NPD 2810, NASA NPD 1000.0) describes a high-level security strategy that points to an overarching risk management framework process (e.g., CNSSI 1253, NASA NPR 2810, NASA NPR 7150.2E) which specifies a "control baseline" using the Low-Moderate-High watermark approach. The control baseline with high-level guidelines is usually where the guidance stops. The control baseline puts the burden on each system designer to decompose the control baselines text into implementable technical requirements.



ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions			X			X			
AC-2(12)	Account Management | Account Monitoring /	+	+	X	+	+	X			

Control Tag	Requirement Text
AC-11	1: The system shall prevent further access to the system by initiating a session lock after [30 minutes] of inactivity or upon receiving a request from a user. {AC-11}
AC-11	3: The system shall ensure that the period of inactivity shall be no more than [30 minutes] before session lock occurs for remote sessions and releasing the session lock requires user re-authentication. {AC-11}
AC-11	3: The system shall ensure that the period of inactivity shall be no more than [30 minutes] before session lock occurs for mobile devices and releasing the session lock requires user re-authentication. {AC-11}
AC-11	2: The system shall retain the session lock until the user reestablishes access using established identification and authentication procedures. {AC-11}
AC-11	1: The Program shall require users to initiate a session lock of information system workstations before leaving them unattended.{AC-11}

Figure 3: Policy vs Controls vs Requirements

Leveraging lessons learned from past implementations and interpretations of the control baselines levied from documents like CNSSI 1253, it is recommended we move from high level generalized guidelines into translated technical security requirements that provide the system designers with a spacecraft specific translation of the control baseline overarching principles. When the translation has been left to system designers, history has shown that many contractors/system designers will analyze the control baselines through an uninformed interpretation of the control text. This leads to many controls and subsequent requirements being "not applicable to spacecraft" or implemented in a way that is not countering actual threats. This usually is a result of semantic differences where tradition control terminology is interpreted verbatim without deciphering the underlying security principles applying to a spacecraft.

These observations are not advocating that every space system should require the same level of cybersecurity protection. Instead, an approach should be adopted where there is an improved common baseline of agreed upon primary security principles that every space system should implement for protection (e.g., authentication, encryption, software assurance, cyber situational awareness). Without this approach, civil and likely commercial space systems will not even consider minimum protections to counter common threats. The method this paper advocates is to accomplish these primary security principles based on threat-informed analysis of controls necessary to mitigate common top risks.

1.3 Threat-Based Risk Management

As structured governance and standards are not available for these new considerations, this paper discusses a threat-based approach for cyber risk management in space systems that can yield effective baseline requirements. Cyberattacks on space systems could come in many ways and depend on the adversary's access, adversary's goals, and the space mission's purpose. There are several categories of space missions that could garner the attention of a nation state. Missions in direct support of military/intelligence, missions that could be leveraged as a utility to an adversary (e.g., stealing mission data, leveraging a sensor), a mission that supports a United States national critical functions, or missions with basic guidance and thruster systems could be used as a kinetic threat to harass, if not collide with, another spacecraft. In the most generic sense, attacks could result in a breach of the system's confidentiality, integrity, or availability and each would have unique impacts on the target system response. A defense-in-depth approach is advocated to implement overlapping protections that will prevent a single compromise causing a full system compromise and to hinder attacker efficiency.

An example depiction of cyber threat vectors for space systems is visually represented in Figure 4. The green lines indicate normal expected communications/access where the red lines indicate communications from adversary's infrastructure directly. Attacks can occur from the mission's own ground infrastructure, adversaries' ground infrastructure, a spacecraft, or via a hardware or software supply chain implant. While the likelihood of each attack path varies depending on adversaries' capabilities, intent, and engineering difficulty, using defense-in-depth principles alongside risk management strategies will aid in countering threats. This approach is supported by SPD-5, "space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering."

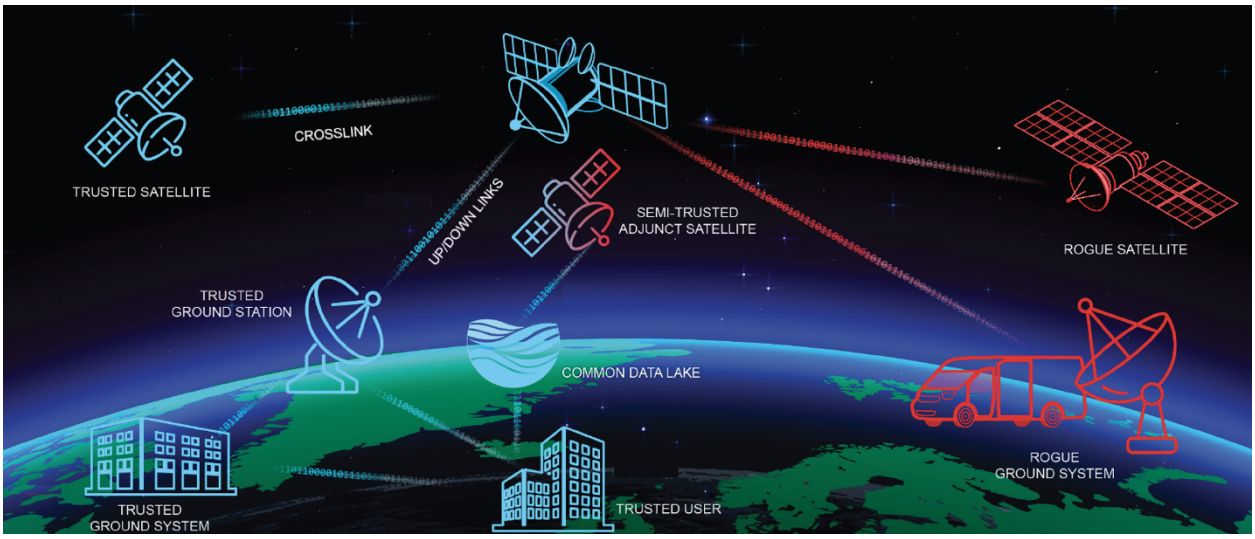


Figure 4: Overview of Cyber Threat Vectors for Space Systems

2 Space Systems Defense-in-Depth

At the most basic level, a spacecraft and the associated ground station can be viewed as two computers networked together over a wireless link. Both are required for the space system to operate correctly. Therefore, a successful cyberattack on either may significantly impact the overall system. One of the fundamental problems with space system design is an assumption that protection at the boundaries will be enough. For space, the boundary is often thought to be the communications link (i.e., radio frequency link) and/or the ground system in general. Little internal protection exists if the boundary is breached. Similar schools of thought existed in the beginning days of traditional cybersecurity, where border firewalls were providing the only protection from intrusion. This approach proved to be faulty, and well-protected IT systems are now designed with defense-in-depth principles. Similarly, current, and future space system designs must overcome the risk of an adversary breaching the boundary and operating unhindered inside the system. Both large traditional developments and more modern rapidly developed space systems should ensure that they have a cyber-hardened design with defense-in-depth throughout. When cybersecurity protections have been deployed, the focus has commonly been on the ground segment with little research or guidance on securing the space segment (i.e., spacecraft). A space system should have cybersecurity protections applied to both the ground and space segments. Figure 5 depicts a visual representation of the layers where defenses can be applied. The outer layer, prevention, is where protection such as governance, supply chain protection, and risk management occur. The inner layers are where the mission data and the flight software reside with protections such as encryption and software assurance to reduce risk.

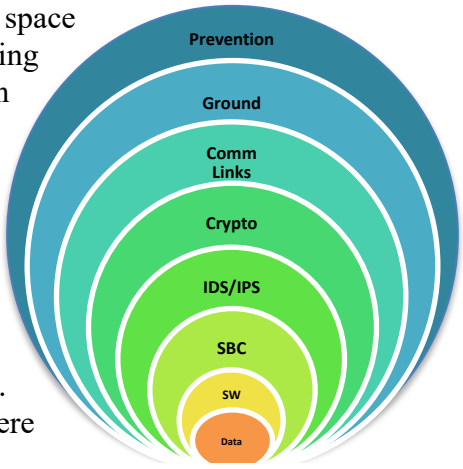


Figure 5: Defense-in-Depth Layers

Recalling the earlier cyber threat graphic in Figure 4 and applying a defense-in-depth strategy, security controls should also be applied at the user segment, ground segment, link segment, and space segment to ensure the space system has a robust security architecture. The next sections outline how to apply defense-in-depth on the space segment only. Ground and wireless link architectures are beyond the scope of this paper.

2.1 Assumed Spacecraft Protection

Many assume that government satellites are generally well protected against cyberattack. In contrast, commercial satellites are generally thought to be more vulnerable [10]. This assumption is made because commercial satellites do not require the same level of governance as government satellites, and they do not have standardized security. In actuality, both assumptions are misplaced and there are challenges across all sectors. In addition, complacency and misunderstandings about spacecraft cyber vulnerabilities have been widespread. In all sectors spacecraft have been built assuming a very limited range of cyber threats. Most spacecraft architectures, subsystems, and supply chains were developed before current cyber threats were envisioned.

To elaborate on the assumption that government owned and operated spacecraft are more immune to cyberattack, these are some of the common rationales provided:

- Spacecraft architectures are built using unique hardware/software that is not susceptible to common computer malware.
- Spacecraft only have communications with protected ground infrastructure that is "air gapped" from the commercial internet, so they cannot be attacked by external adversaries.
- Physical access to spacecraft once launched is highly unlikely.
- Some spacecrafts are developed, manufactured, and launched by cleared defense contractors, with closed supply chains that are not accessible by potential adversaries.
- Strong National Security Agency (NSA)-approved encryption on spacecraft uplinks/downlinks means that data cannot be exposed to or manipulated by adversaries.

When considering the current space environment, these assumptions have significantly eroded.

- Through maturation of attack methods and emerging proliferation of common spacecraft bus architectures, there has evolved a common set of attack methods (i.e., tactics, techniques, and procedures) for attacking spacecraft. For example, there are openly published papers for attacking the MIL-STD-1553 communication bus, which is used in many spacecrafts. [11]
- The protection provided by an airgap has significantly been reduced by many successful attack methods bypassing this protection. For example, the are many documented attacks on air-gapped ICS systems. [12]
- Remote proximity operations and on-orbit docking are being matured, which can be used for malicious attack. [13]
- Supply chain risk management has become a critical issue for government systems and commercial contractors are a target. The most recent and significant supply chain compromise was the Russian intelligence compromise of the SolarWinds Orion Platform. [14]
- Not all government systems in operation have current NSA-approved encryption or encryption at all. It was not until the publication of NASA-STD-1006 in 2019 where NASA began requiring standardized encryption for NASA missions which is based on Federal Information Processing Standard 140, Security Requirements for Cryptographic Modules, Level 1. [15]

2.1.1 Common Spacecraft Cybersecurity Gaps

As an expansion to the earlier defense-in-depth graphic, Figure 6 provides a breakout of spacecraft security principles that can aid in resilience and cyber protections. For the spacecraft, most security is geared around cryptography on the command link, Transmission Security (TRANSEC), and some Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST) controls. The items highlighted in red are where cyber gaps most likely reside:

- **S/C Software:** Software assurance principles are a challenge with existing software systems and are much less likely to be applied for spacecraft software
- **SBC and IDS/IPS:** There are little to no security-security focused capabilities for on-board monitoring, logging, and alerting
- **Crypto:** Some systems have crypto failure "safe modes" that can put spacecraft in a vulnerable state (i.e., crypto bypass mode)

- **Ground:** Capabilities are immature for monitoring ground system compromise for malicious commanding to the satellite.
- **Prevention:** Supply chain risk management continues to be a challenge and there are insufficient satellite-focused cybersecurity policies and procedures. Insider threats are also rarely considered and often considered to be mitigated by personnel security/background checks but it takes cyber controls in addition to the personnel ones to effectively reduce insider risk.

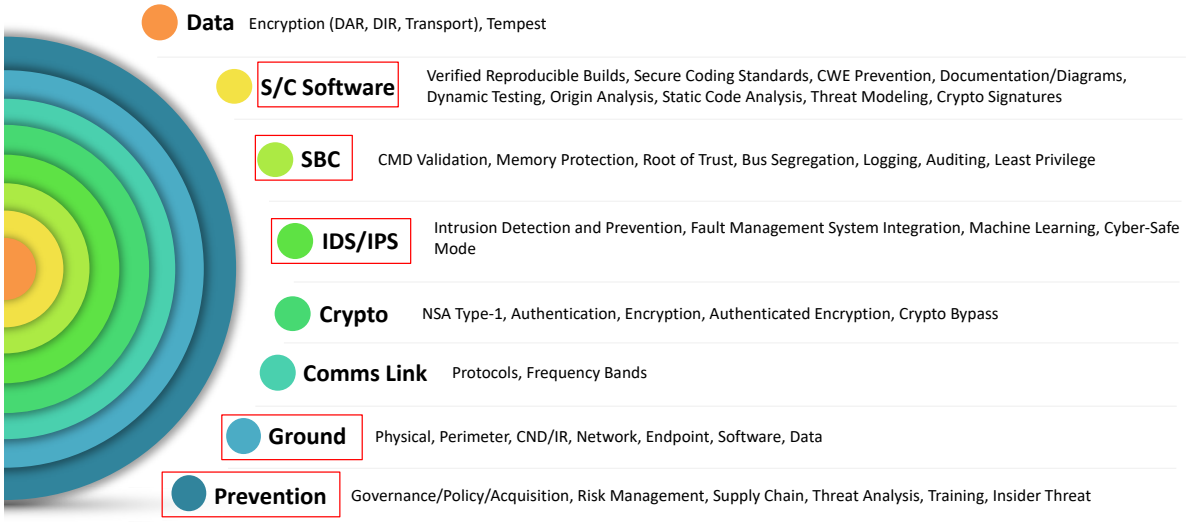


Figure 6: Defense-in-the-Depth Overview for Space Systems

2.1.2 Defense-in-Depth Security Principles for Spacecraft

A further expansion of Figure 6 is depicted in Table 2, which outlines layers and sub-categories in more granular detail. These security principles should be thought of as a menu of options and a threat/risk analysis is needed to determine where the system designer should spend time and effort deploying the controls. The sub-categories denoted with * could be controls implemented during development/sustainment in addition to operational controls. Additionally, from a governance perspective on legacy and future space systems, organizations can use this table to validate whether the spacecraft has incorporated these security principles in design. Further decomposition in the ground layer for defense-in-depth is provided under separate analysis.

Table 2: Expanded Defense-in-Depth for Space Systems

DiD Layer	DiD Sub-Layer	Implementation Goal
Data	**Encryption (DAR, DIT, transport, etc.)**	Ensures confidentiality and integrity at rest or in transit (within the spacecraft) for all critical data.
	Tempest	Shielding sensitive equipment from emanating electromagnetic radiation that may carry sensitive information. Applied to prevent the information from being intercepted by outside entities.
S/C Software	**Configuration Management (CM)/Build Environment***	Build environment is reproducible and verifiable (e.g., software bill of materials validation) throughout the build process. Stringent source code control with strong authentication (e.g., multi-factor) on software

DiD Layer	DiD Sub-Layer	Implementation Goal
		commits. Build system needs to be deterministic where the source code always produces the same resulting build.
	Secure Coding Standards*	Secure coding standards identified in policy. AND Standards are enforced during implementation (e.g., violation alerts in IDE, manual code review, etc.).
	Common Weakness Enumeration (CWE) Prevention*	Performs own system-specific scoring of CWEs for prioritization of which weaknesses will have the highest impact on the spacecraft given how the software operates.
	Documentation/Diagrams (deployed location, I/O, data types, etc.) *	Maintains high-level documentation of software architecture with data flows defined. AND Maintains lower-level diagrams of input/output modules with data types handled by each.
	Dynamic Testing*	Performs continuous dynamic testing throughout flight software development, operations, and maintenance.
	Software Component Analysis (i.e., Origin Analysis) *	Maintains complete knowledge of software components utilized in flight software (e.g., software bill of materials). AND Tracks all associated vulnerability information for the components.
	Static Code Analysis*	Performs static analysis scans with a complimentary set of tools. AND has a defined process for prioritization/remediation of security related findings.
	Threat Modeling*	Adheres to a formal software threat modeling process following an established framework (or custom developed equivalent).
	Crypto Signatures/Code Signing	Lightweight cyber protection functions implemented (e.g., hashes), and best practices applied in subsystems/firmware throughout the spacecraft to assure the software author and guarantee that the code has not been altered or corrupted since it was signed. Software and firmware updates verified with cryptographic signatures/code signing. Cryptographic signatures provide the means to protect the integrity of the content and to verify its authenticity.
SBC/Bus/ Processor	**CMD Validation**	All received commands have authentication and validation. Appropriate counters are used for both valid and invalid commands.
	Memory Protection	Memory monitoring and protection solution is efficiently used and configured.
	Root of Trust (RoT)	RoT trusted computing module implemented on radiation tolerant burn-in (non-programmable) equipment. RoT functions, such as verifying the device's own code and configuration, must be implemented in secure hardware.
	Bus Segregation	Communication buses which bridge critical and non-critical spacecraft systems should either be separated or explicitly protected. Shared bus communication between components that cannot be separated should have countermeasures applied at each component's interface (e.g., encryption, authentication, babble protections).
	Logging	Collection and storage of data over a period of time to analyze events/actions of the system, such as interactions through which data, files, or software is stored, accessed, or modified. The spacecraft should independently perform command logging and anomaly detection of command sequences for cross validation.
	Auditing	Security audits of logs are part of the mission's security plan/policies/procedures. AND Security audits are efficient and executed as planned.
	Least Privilege	OS tasks run in the context of least privilege and a zero-trust approach is used with flight processor software.
IDS/IPS	**Intrusion Detection and Prevention**	Continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. Implementation of both signatures based and algorithm/machine learning-based anomaly detection techniques.
	Fault Management System Integration	IDS and fault management systems should be integrated as they are performing similar functions but looking for different anomaly

DiD Layer	DiD Sub-Layer	Implementation Goal
		signatures. Consideration should also be included to avoid conflicting actions between the two systems.
	Machine Learning	Automation should be trained on a data set that includes a variety of typical system operations and undergoes adversarial attack methods. Space operations are highly structured and in general lend themselves well to machine learning for anomaly detection.
	Cyber-Safe Mode	The spacecraft IPS and the ground should retain the ability to return spacecraft critical systems to a known cyber-safe mode where all non-essential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. The default cyber-safe mode software should be enabled by the RoT hardware.
Crypto	**NSA Type-1**	A Type 1 product is a device or system certified by the NSA for cryptographically securing confidentiality of classified U.S. Government information. Type-1 is usually only applicable to National Security Space missions. The term “Type 1” also refers to any cryptographic algorithm (or “Suite,” as NSA refers to them) that has been approved by NSA for use within Type 1 equipment.
	Authentication (w/o Encryption)	Authentication, integrity, and the anti-replay function on the space communication link when data confidentiality is not required. Authentication for spacecraft commands provides assurance that the spacecraft can only be controlled/commanded by an authorized control center.
	Encryption (non-Type-1 w/o Authentication)	Provides data confidentiality but no authentication or integrity. Encryption primitives transform a block of plaintext data into ciphertext data. Encryption-only for a particular use case does not protect against malicious manipulation of data.
	Authenticated Encryption (non-Type-1)	Combination of encryption and authentication, thus, providing data confidentiality, data integrity, authentication, and anti-replay function. Authenticated encryption algorithms combine authentication and encryption algorithms with a single cryptographic key and algorithm.
	Crypto Bypass	Crypto bypass is completely disabled. All communication is properly encrypted.
Comms Link	**Protocols**	Communications protocol designed to be used over a space link, or in a network that contains one or multiple space links. A space link is a communications link between a spacecraft and its associated ground system or between two spacecraft. Protocols should include the capability to support security principles like authenticated encryption within the protocol.
	Frequency Bands	Having resilient communication uplink methods such as multiple paths, frequency hopping, or spread spectrum.
Ground	**Physical**	Traditional physical security controls for a physical location, such as badge control, fire suppression, guards/gates/guns with proper surveillance.
	Perimeter	Ground infrastructure has proper firewall configurations, data loss prevention, and security zones for external interactions (i.e., DMZ).
	Computer Network Defense/Incident Response (CND/IR) *	Robust architecture is established with threat hunting, intrusion detection/prevention, targeted sensor placement with TAPs and SIEMs. Security operations center functions with documented procedures and policies to detect, respond, and recover.
	Network	Employment of least-trust principles with protection such as access control lists, segmentation, port security, and communication authentication.
	Endpoint*	Hardening of endpoint devices such as two-factor authentication, host-based intrusion detection/protection, anti-virus/malware, patching and vulnerability scanning.
	Software*	Utilization of software assurance methods for all ground system software. Procedures and tools are available to prevent CWEs and

DiD Layer	DiD Sub-Layer	Implementation Goal
		eliminate CVEs as well as tracking software bill of materials. Dynamic analysis in space-centric cyber test beds is performed.
	Data*	Data-at-rest and data-in-transit encryption is utilized, TEMPEST is deployed, Operations Security (OPSEC) is practiced, permissions and access control are applied to all sensitive data.
Prevention	**Governance / Policy / Acquisition***	Cybersecurity requirements are established in overarching policies and flow down into acquisition for contractors to implement.
	Risk Management*	Integration of cyber threat risk assessment with overall concepts of risk management during requirements creation. Infusion of cyber resilience and concepts into the initial stages of concept development enables trades of possible mitigations or alternative architectures. Leverage adversary simulation and digital twin technologies to perform technical security testing at the system level. More technical analysis and testing should be included in the risk management and approval process.
	Supply Chain*	Establish supply chain risk management program for hardware and software suppliers. Critical components and subsystems should be identified and handled with prioritization to mitigate primary impacts to the system.
	Threat Analysis*	Ability to gather and analyze threat intelligence against the system.
	Training*	Regular role-based cyber training occurs at regular intervals. For example, mission operators need to perform threat hunting or red versus blue events where defensive cyber operators learn how to detect, respond, and recover from cyberattacks.
	Insider Threat*	While defense-in-depth will aid in mitigating insider threat to a degree, a formalized insider threat program is warranted in many cases to ensure dedicated resources and training are available.

2.1.3 Integrating Security Principles in Existing Policy

Government funded spacecraft have not always used security guidelines like NIST and/or CNSSI 1253. When they have, Aerospace observations have been that there are significant oversights and gaps in spacecraft security implementation. Unlike ground systems, spacecraft may not follow an authorization process such as the Risk Management Framework or an agency equivalent policy to achieve an authorization to operate (ATO). Programs and/or organizations have attempted to take portions of NIST governance and apply it to spacecraft. The most notable attempt at this was with CNSSI 1253 and the generation of the space overlay in appendix F. The space overlay was an attempt to take an existing control set and create an overlay specific for the spacecraft and launch vehicle. The concept of a security overlay is to take an existing set of security controls (e.g., CNSSI 1253, NIST SP 800-53) and tailor applicability to the specific system context. For the space overlay, the authors took the existing control set and articulated generally what could be applicable to the spacecraft. A deficiency in this approach is that the results are not directly informed by current threats and just indicate general applicability that is difficult to interpret for specific implementation details. The CNSSI 1253 space overlay has a purpose for starting basic spacecraft protection, but an improvement to this approach is to link controls more specifically to threats under risk assessment and provide control implementation details specific to a spacecraft.

Translating generalized control terminology (e.g., organization shall, information system shall) into more technical security requirements focused on spacecraft will leave less room for incorrect interpretation and implementation. The below example is a simple requirement derived from the IA-3 control which should apply to any spacecraft. This requirement is one of several that would help mitigate an adversary attempting command link intrusion and replay attacks via the ground or via cross-link communications.

> ***NIST SP 800-53r4 IA-3:*** The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.
>
> 
>
> ***Translation:*** The spacecraft shall uniquely identify and authenticate the ground station and other spacecrafts before establishing a remote connection.

It should specifically be noted that the effort here to provide more specific terminology is not an attempt to be constraining and prescriptive to the designer. Instead, this specificity should be interpreted as guidance that can be tailored appropriately for the system. These definitions point the design in the right direction for what is likely necessary to combat current threats.

According to OWASP, a security requirement is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied. Security requirements are derived from industry standards, applicable laws, and a history of past vulnerabilities. Security requirements define new features or additions to existing features to solve a specific security problem or eliminate a potential vulnerability. Security requirements provide a foundation of vetted security functionality for an application. Instead of creating a custom approach to security for every application, standard security requirements allow developers to reuse the definition of security controls and best practices. Those same vetted security requirements provide solutions for security issues that have occurred in the past. Requirements exist to prevent the repeat of past security failures. [16]

While OWASP was established for web application security, their definition for security requirements is very accurate and applicable for designing and developing a secure space system. When attempting to generate a requirements baseline, creators should start from a clean sheet of paper to establish the specific baseline. With this approach, designers/engineers can take a master catalog of security guidelines (i.e., CNSSI 1253 / NIST SP 800-53 and all the enhancements) and generate their system baseline. While baseline generation can be labor intensive, it will result in tailored controls/requirements for a particular mission.

In order to create an appropriate baseline, the engineers need to understand the applicable threats during requirement derivation. Performing an in-depth analysis of every known cyber threat can be time consuming; however, leveraging previous Aerospace work, an unclassified listing of cyber threats for a space system was published in October 2020 [17]. As necessary, this threat information can be augmented with additional information from classified sources or specific threats to the system under development.

The generic threat library depicted in Figure 8 was produced by interviewing subject matter experts and reviewing many publications for threats, vulnerabilities, requirements, and security principles. Figure 7 depicts a sampling of the resources reviewed to curate the threat library and associated security principles to mitigate.

DoD / Government Resources:
CNSSI 1253 Space Overlay
GPS RMF002 Requirements
HPSC Cyber Secure Boot Requirements
MDA Software Assurance Overlay version 19-MDA-10112 (19 Jun 19)
DARPA – System F6 Tech Package (F6TP)

Civil Space:
NOAA ITSM and FIPS documents
NASA Candidate Protection Strategies v4 – November 4, 2019
NASA Software Safety Standard and Handbook – NASA-STD-8719.13

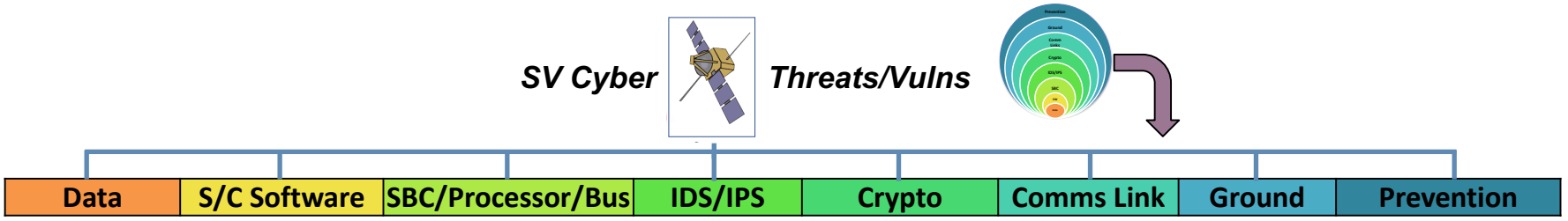
Aerospace Curated Data:
Aerospace CSPS – Defending Spacecraft in a Cyber Domain
Watcher Presentations/Papers
TOR-2019-02178 – Telemetry Security
TOR-2018-02275 – A Need for Robust Space Vehicle Cybersecurity
TOR 2018-01164 – Space-Cyber Requirements for Future Systems
TOR-2019-00506 (ASIC/FPGA Assurance) Rev A Spreadsheet v1-2
Aerospace SCRM TOR Under Development

Open Source / Commercial Resources:
CCSDS Threat Green Book (updated draft not yet released)
CENTRA Tech. – Cyber Content of Satellites
CENTRA Tech. – Cyber Threats to Satellite Networks
CENTRA Tech. – Cyber Threats to Satellite-Based IP Networks
CENTRA Tech. – Chinese Research – Satellite Bus Vulnerabilities
CENTRA Tech. – Foreign Satellite Developers Design & Cyber Content
Orbital Security – Space Cyber Guidelines for Commercial Satellites rev-1.0.1
NIST 800-53 Rev 4
Cybersecurity for Space: Protecting the Final Frontier (rel. March2020)

Figure 7: Referenced Material Reviewed for Threat Library

Engineers can leverage this generic threat library to help identify likely threats that will drive the security requirements baseline. Space systems will likely have additional threats to consider, but the below depiction is a starting point for generating a security baseline. Figure 8 establishes a library of layer-based threats and vulnerabilities applicable to a space system that should be considered for mitigation during design and/or operations.

It should be noted that the authors acknowledge that there is difference between threats and vulnerabilities under risk assessment methodologies. However, the content extracted from the sources did not formally distinguish between these aspects and the intent is to reference the wording as stated by the source. An effort to distinguish between threats and vulnerabilities would end up unnecessarily complicating the analysis and would ultimately not change the risk assessment process advocated. As described in subsequent content, risk assessment will be accomplished through likelihood and impact determinations. Ultimately the aspects of threat and vulnerability combine into a likelihood rating and the need for separate definition effectively becomes moot.



SV-AC-3 Compromised master keys or any encryption key

SV-IT-2 Unauthorized modification or corruption of data

SV-CF-2 Eavesdropping (RF and proximity)

SV-MA-2 Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyber attacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning

SV-SP-1 Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW.

SV-SP-3 Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse

SV-MA-3 Attacks on critical software subsystems {AD&C, TT&C, C&DH, EPS}

SV-SP-6 Software reuse, COTS dependence, and standardization of onboard systems using building block approach with addition of open source technology leads to supply chain threat

SV-AV-4 Attacking the scheduling table to affect tasking

SV-IT-5 Onboard control procedures (i.e. ATS/RTS) that execute a scripts/sets of commands

SV-SP-9 On-orbit software updates/upgrades/patches/memory writes.

SV-AC-5 Proximity operations (i.e. grappling satellite)

SV-AV-2 Cyber attack to disrupt timing/timers could affect the vehicle (Time Jamming / Time Spoofing)

SV-AC-6 Lack of bus segregation (e.g. 1553 injection). Things are not containerized from the OS or FSW perspective

SV-AV-3 Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol

SV-IT-3 Compromise boot memory

SV-IT-4 Cause bit flip on memory via single event upsets

SV-SP-7 Attacking the on-board operating systems. OS has a critical role in the overall security of the system.

SV-AV-8 Clock synchronization attack for Spacewire.

SV-AC-8 Malicious Use of hardware commands - backdoors / critical commands

SV-MA-8 Payload (or other component) is told to constantly sense or emit or run whatever mission it had to the point that it drained the battery constantly / operated in a loop at maximum power until the battery is depleted.

SV-SP-11 Software defined radios cyber attack

SV-AV-5 Using fault management system against you. Example, safe-mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of RPO to cause S/C to go into safe mode;

SV-AV-6 Complete compromise or corruption of running state

SV-DCO-1 Not knowing that you were attacked or attack was attempted

SV-MA-5 Not being able to recover from cyber attack

SV-IT-1 Communications system spoofing resulting in denial of service and loss of availability and data integrity

SV-CF-1 Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determine which entities are communicating with each other without being able to read the communicated information

SV-AC-1 Attempting access to an access-controlled system resulting in unauthorized access

SV-AC-2 Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction

SV-CF-4 Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack

SV-AV-1 Communications system jamming resulting in denial of service and loss of availability and data integrity

SV-AC-7 Weak communication protocols. Ones that don't have strong encryption within it

SV-MA-7 Exploit ground system and use to maliciously to interact with the SV

SV-AC-4 Masquerading as an authorized entity in order to gain access/Insider Threat

SV-SP-2 Testing only focuses on functional requirements and rarely considers end to end or abuse cases

SV-SP-4 General supply chain interruption or manipulation

SV-MA-1 Space debris

SV-SP-5 Hardware failure (i.e. tainted hardware) {ASIC and FPGA focused}

SV-CF-3 Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored Unclass or on contractors network

SV-AV-7 TT&C in first 10 years leads to most faults; degradation of moving parts follows (gyro, momentum wheels, etc.); then attitude control being other threat

SV-MA-4 Not knowing what your crown jewels are and how to protect them now and in the future.

SV-SP-10: Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3 and SV-SP-4)

SV-MA-6 Not planning for security on SV or designing in security from the beginning

Figure 8: Space Cyber Threats/Vulnerabilities for Space Systems

3 Threat Informed Requirements for Spacecraft

When improving a legacy system or designing a new cyber resilient space system, many different security control implementations exist that will improve space systems' security. Thorough risk management processes should drive the selection of which defense-in-depth principles to employ. To manage risk, decisionmakers should assess the likelihood and potential impact of a cyberattack against the space system and then determine the best approach to deal with the risks: avoid, transfer, accept, or mitigate. To mitigate risks, decision makers must ultimately determine which defense-in-depth principles (i.e., security requirements) apply. Not all risks can be eliminated, and no decisionmaker has unlimited budget or enough personnel to combat all risks.

Every program will need to perform their own risk assessment considering threats, vulnerabilities, impact, and mitigating requirements. NIST SP 800-154 provides guidance on using data-centric system threat modeling as a method for determining applicable threats and the necessary mitigating controls. A similar process is outlined in this section as a representative example to aid others in performing this analysis. Agencies, programs, and companies may have their own risk assessment process that can be used as needed, but this paper describes a simplistic risk analysis approach using a 5x5 risk matrix. The acceptable level of risk (i.e., risk tolerance) will be mission dependent. Security requirements can be reduced as mission importance is factored in and likewise the overall risk tolerance increases (e.g., defense critical asset vs. research demonstration).

3.1 Threat Terminology

Definitions are a key to understanding the process for deriving which risks, threats, and vulnerabilities must be addressed. Definitions are adapted from RFC 4949 – Internet Security Glossary v2 [14], and the Committee on National Security Systems (CNSS) Glossary [15].

> *Threat:* Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation.
>
> *Threat Action:* A realization of a threat, i.e., an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act. (e.g., sending malicious inputs)
>
> *Threat Agent (a.k.a. adversary):* A system entity that performs a threat action, or an event that results in a threat action.
>
> *Vulnerability*: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
>
> *Exploit*: A technique or process to take advantage of the vulnerability.
>
> *Risk*: A measure of the extent to which an entity is threatened by a potential circumstance or event. Principally the combination of threat, vulnerability, and the exploit.

Attack: An intentional act by which an entity attempts to evade security services and violate the security policy of a system.

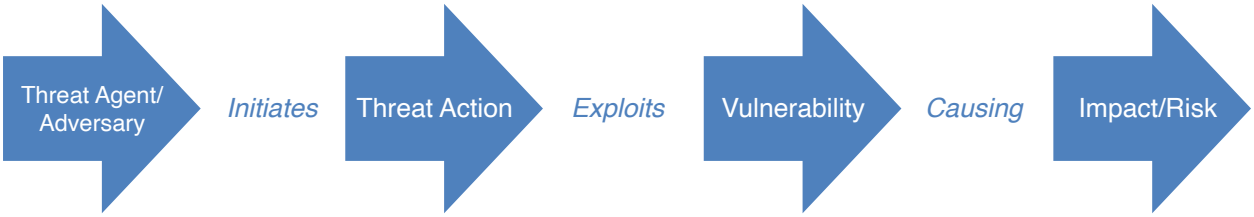


Figure 9: Relationship Between Terms

3.2 Space Specific Cyber Threat Model

With risk assessment as the backdrop, the subsequent example process can be used to establish a threat and risk informed space system baseline. Note that the goal here is a baseline vice a control overlay as was previously discussed. Keep in mind that in an ideal scenario this would need to be completed for each program using mission specific threat intelligence and mission design to better classify impact and likelihood. However, using a pre-defined, tiered adversary system to calculate likelihood in combination with an unclassified threat model, an example security baseline can be established. Cyber threat likelihood includes aspects such as exploitation difficulty, motivation, and adversary capabilities. The motivation and exploitation difficulty would be program dependent, but the adversary capabilities can be analyzed using a generic approach. Using a space specific threat model influenced by *Adversary Threat Model for Requirements, Acquisition and Cybersecurity Engineering* [20], Figure 4 cyber threat vectors can be updated with applicable adversary threat tiers as depicted in Table 3.

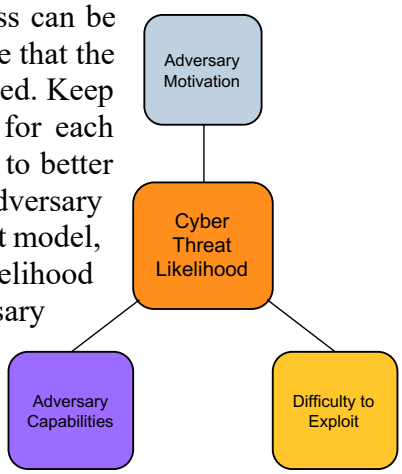


Figure 10: Cyber Threat Likelihood

Table 3: Threat Agents in Cyber Threat Model

Tier	Name	Skills	Maliciousness	Motivation	Methods
I	Script Kiddies	Very low	Low	Boredom, thrill seeking	Download and run already-written hacking scripts known as “toolkits”
II	Hackers for Hire	Low	Moderate	Prestige, personal gain, thrill seeking	Write own scripts, engage in malicious acts, brag about exploits
III	Small Hacker Teams, Non-State Actors OR Disorganized/Non-Advanced State Actors	Moderate	Moderate	Power, prestige, intellectual gain, respect	Write scripts and automated tools

Tier	Name	Skills	Maliciousness	Motivation	Methods
IV	Insider Threats (e.g., disgruntled employees)	Very Low – Very High	Very Low – Very High	Unwitting, ideology, politics, espionage	Insider knowledge lowers the barrier of entry. Methods span the spectrum from simple to sophisticated.
V	Large, Well-Organized Teams, Criminal, Non-State, or State Actors	High	High	Personal gain, greed, revenge	Sophisticated attacks by criminal/thieves, may be "guns for hire" or involved in organized crime
VI	Highly Capable State Actors	Very high	Very high	Ideology, politics, espionage	State sponsored, well-funded cyberattacks against enemy nations
VII	Most Capable State Actors				

In this threat model, each tier was evaluated for capabilities around:

- Ability to Access Networks
- Ability to Discover & Exploit Vulnerabilities
- Ability to Defeat Crypto & Authentication
- Command & Control Sophistication
- Ability to Affect Cyber/Physical Systems
- Ability to Gain Physical Access
- Sophistication of Human Influence

The resulting analysis is reflected in an updated threats vectors diagram with a threat tier overlay as shown in Figure 11. This diagram can assist in understanding the adversary levels a program could face for specific threat vectors. Not every program will have to be resilient and mitigate threats across Tier I-VII. For example, a program may have a 90-day mission with a small budget and may choose to accept the risk that a Tier IV-VII adversary could successfully end their mission. This program will still want to mitigate threats vectors tied to Tier I-III. A notional mapping of the threats from Figure 8 to the threat tiers in Table 3 is provided in Appendix A, Table 5.

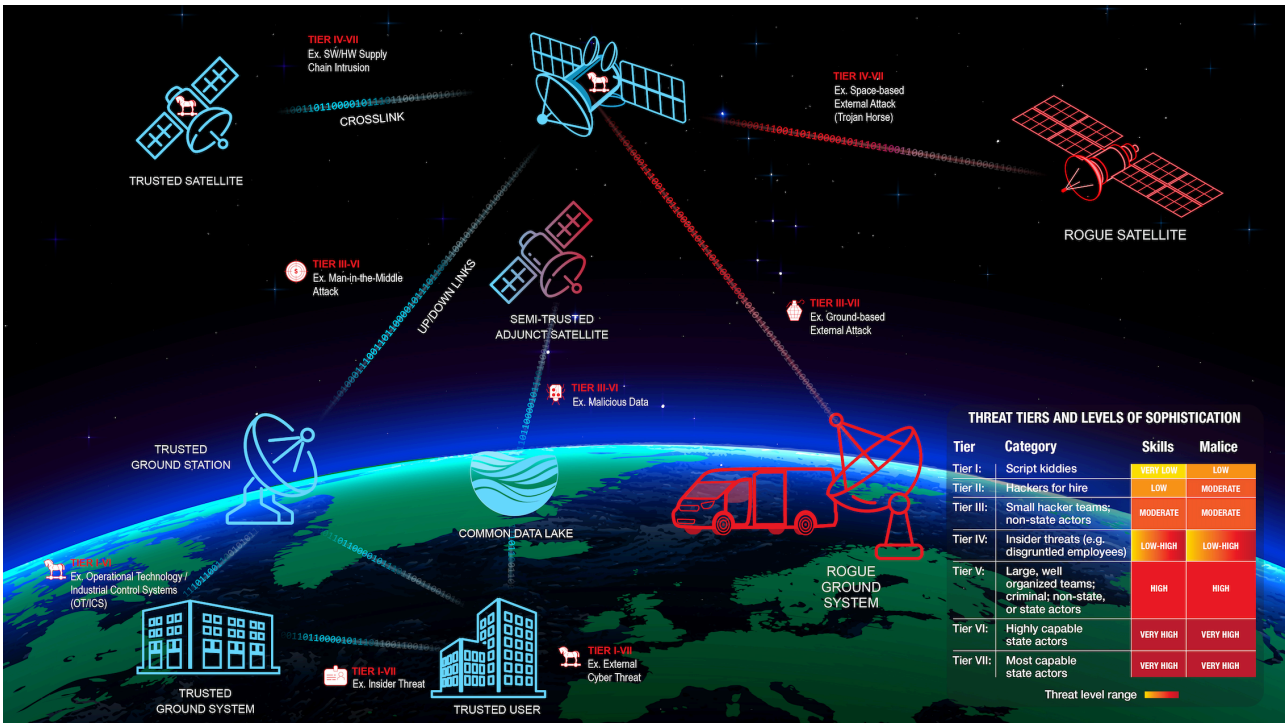


Figure 11: Attacker Tiers Overlaid on Cyber Threat Vectors for Space Systems

3.3 Ranking Threats on a 5x5 Risk Matrix

Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:

- the adverse impacts that would arise if the circumstance or event occurs; and
- the likelihood of occurrence (NIST SP 800-30) [21]

The purpose of a risk assessment is to identify & evaluate risks to the mission and can be used to guide prioritization of mitigations, both design/implementation and procedural, and candidates for requirements. Space systems are a combination of traditional-IT components (e.g., ground systems, software), operational technology (e.g., industrial control systems), and spacecraft platforms (e.g., satellite bus). Risk to traditional-IT components & operational technology components is better understood than spacecraft risks. Applying traditional-IT based methodologies such as the NIST Risk Management Framework (RMF) to platforms has had mixed results, as previously discussed. Therefore, the focus of the subsequent sections will be using threats agents, threat actions, vulnerabilities, and risk to derive technical security requirements.

Using the previously described threat model, impact and likelihood can be calculated and placed on a traditional 5x5 risk matrix where the most critical threats/risk appear in the upper right-hand corner of the matrix. This space specific threat model can be used for legacy space systems to identify current risks as well as for future deployments to identify potential future risks that can be mitigated via secure design choices. Below is a visual depiction of an example ranking on a 5x5

risk matrix using the predefined threats/vulnerabilities from Figure 8. This analysis was performed assuming a rather simple ground to space architecture in low earth orbit with no predefined security requirements. This analysis resulted in a many common threats and vulnerabilities that a traditional low earth orbit mission would be exposed to.

ID	Threat/Vuln Category	Max Impact	Likelihood	Essential	Rank	
SV-AV-1	TT&C Security	5	5	x	25	Communications system jamming resulting in denial of service and loss of ava
SV-IT-1	TT&C Security	5	5	x	25	Communications system spoofing resulting in denial of service and loss of ava
SV-SP-1	Supply Chain	5	5	x	25	Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, et
SV-AC-7	SV Access Control	5	5	x	25	Weak communication protocols. Ones that don't have strong encryption with
SV-MA-7	SV Mission Assurance	5	4	x	24	Exploit ground system and use to maliciously to interact with the SV
SV-AV-5	SV Availability	5	4	x	24	Using fault management system against you. Understanding the fault respor
SV-AV-6	SV Availability	5	4	x	24	Complete compromise or corruption of running state
SV-AC-2	TT&C Security	4	5	x	23	Replay of recorded authentic communications traffic at a later time with the
SV-MA-6	SV Mission Assurance	4	4	x	22	Not planning for security on SV or designing in security from the beginning
SV-AC-1	TT&C Security	5	3	x	21	Attempting access to an access-controlled system resulting in unauthorized a
SV-AC-3	TT&C Security	5	3	x	21	Compromised master keys or any encryption key
SV-AC-8	SV Access Control	5	3	x	21	Malicious Use of hardware commands - backdoors / critical commands
SV-SP-5	Supply Chain	5	3	x	21	Hardware failure (i.e. tainted hardware) {ASIC and FPGA focused}
SV-MA-5	SV Mission Assurance	5	3	x	21	Not being able to recover from cyber attack
SV-AC-6	SV Access Control	5	3	x	21	Three main parts of S/C. CPU, memory, I/O interfaces with parallel and/or se
SV-SP-11	Supply Chain	5	3	x	21	Software defined radios - SDR is also another computer, networked to other
SV-CF-1	TT&C Security	3	5	x	20	Tapping of communications links (wireline, RF, network) resulting in loss of cc
SV-MA-8	SV Mission Assurance	4	3	x	19	Payload (or other component) is told to constantly sense or emit or run what
SV-AC-4	TT&C Security	4	3	x	19	Masquerading as an authorized entity in order to gain access/Insider Threat
SV-SP-3	Supply Chain	4	3	x	19	Introduction of malicious software such as a virus, worm, Distributed Denial-
SV-SP-4	Supply Chain	4	3	x	19	General supply chain interruption or manipulation
SV-SP-10	Supply Chain	4	3	x	19	Compromise development environment source code
SV-MA-3	SV Mission Assurance	4	3	x	19	Attacks on critical software subsystems* Attitude Determination and Contro
SV-DCO-1	SV Defensive Cyber Operations	3	4		18	Not knowing that you were attacked or attack was attempted
SV-IT-3	SV Integrity	5	2		17	Compromise boot memory
SV-SP-2	Supply Chain	2	5		16	Testing only focuses on functional requirements and rarely considers end to e
SV-CF-3	SV Confidentiality	2	5		16	Knowledge of target satellite's cyber-related design details would be crucial
SV-IT-2	SV Integrity	3	3		15	Unauthorized modification or corruption of data

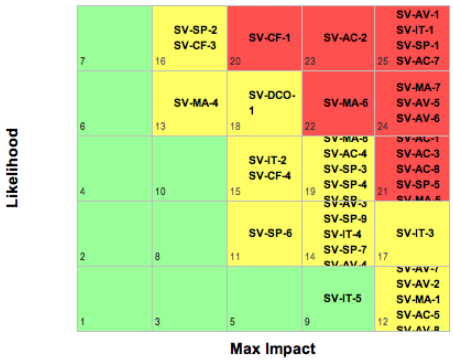


Figure 12: Example Risk Ranking of Cyber Threats

3.4 Prioritizing Cyber Threats for Space

Overlaying this 5x5 risk matrix analysis with the previous graphical depiction of cyber threats, Figure 13 depicts the essential threats/vulnerabilities that should be addressed with the baseline control set or deployment of new mitigations for legacy systems. The items highlighted in red are the most essential to mitigate based on analysis using a space specific threat model that accounted for known adversary capabilities.

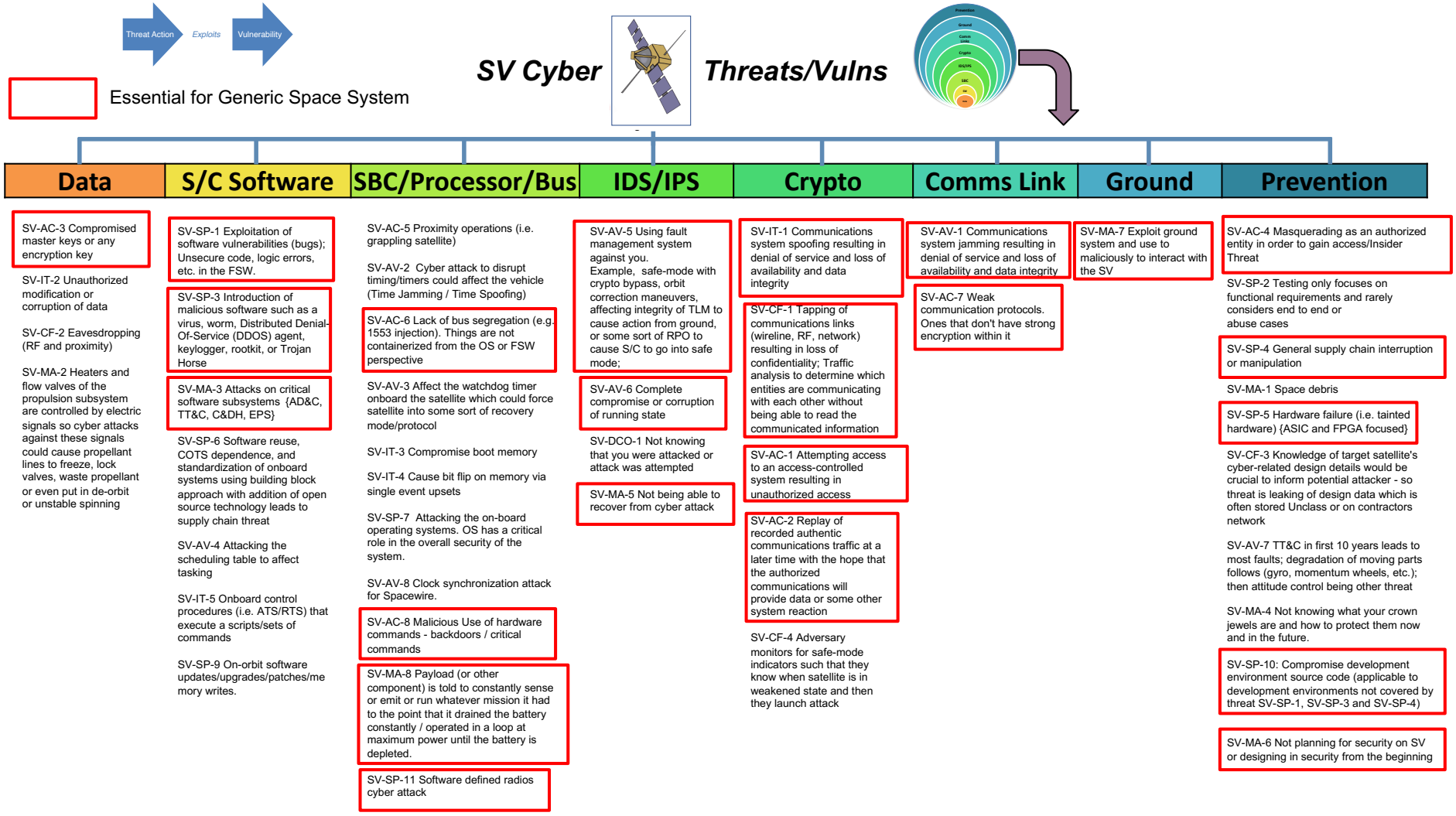


Figure 13: Prioritized Space Cyber Threats/Vulnerabilities for Space Systems

An expansion of the above graphic is listed in the below table to focus solely on the essential threats/vulnerabilities that require mitigation. The categories denoted with * are threats/vulnerabilities that have mitigations needed during development in addition to operations. Table 5 in Appendix A contains more information on each threat/vulnerability.

Table 4: Essential Cyber Threats/Vulnerabilities to Mitigate for Space Systems

Category	Essential Threats / Vulnerabilities to Mitigate for Space
Data	SV-AC-3: Compromised master keys or any encryption key. Encryption is great but self-defeating if key management is not properly implemented.
S/C Software*	SV-SP-1: Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the flight software. Due to autonomy of spacecraft and increased usage of software on-board, software attacks can be mission ending.
	SV-SP-3: Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, rootkit, or Trojan Horse. Outside of unintentional vulnerabilities with on-board software, malicious compromise of the software supply chain is a substantial threat and can be difficult to detect and prevent depending on the sophistication. Malicious logic embedded in software is difficult to detect due to the novel nature of it which can't be detected using signatures.
	SV-MA-3: Attacks on critical software subsystems {AD&C, TT&C, C&DH, EPS}. Many critical components on the spacecraft are controlled by software and adversaries would target these mission critical sub-systems
SBC/Processor/Bus	SV-AC-6: Lack of bus segregation (e.g., 1553 injection). Things are not containerized from the operating system or flight software perspective. Generally, the on-board architectures rely on trust and segregation is often not implemented. While this is a default security principle in traditional IT, it is lacking in most spacecraft architectures.
	SV-AC-8: Malicious use of hardware commands - backdoors / critical commands. Some spacecraft components have built in backdoor commands which can be exploited if discovered. Only enable the required backdoor commands or disable all commands that are not authenticated and encrypted.
	SV-MA-8: Payload (or other component) is told to constantly sense or emit or run whatever mission it had to the point that it drained the battery constantly / operated in a loop at maximum power until the battery is depleted. Power is a critical commodity on the spacecraft and the availability of the spacecraft is directly dependent on power. If not properly implemented, a compromised payload could drain spacecraft power.
	SV-SP-11: Software Defined Radios (SDRs) cyberattack. SDRs are gaining in popularity and capability, these minicomputers are vulnerable to attacks like any other computational component.
IDS/IPS	SV-AV-5: Using fault management system against you. Example, safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of telemetry to cause action from ground, or some sort of proximity operation to cause spacecraft to go into safe mode. Understand your safing procedures and not putting the spacecraft in a more vulnerable state is key to building a resilient spacecraft.
	SV-AV-6: Complete compromise or corruption of running state can be possible if not engineered properly. High integrity controls need to be in place to revert to safe and secure state.
	SV-MA-5: Not being able to recover from cyberattack. Autonomy is required for spacecraft and a well-designed fault management strategy accompanied with the high integrity safe/secure state is crucial.
Crypto	SV-IT-1: Communications system spoofing resulting in denial of service and loss of availability and data integrity
	SV-CF-1: Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determine which entities are communicating with each other without being able to read the communicated information
	SV-AC-1: Attempting access to an access-controlled system resulting in unauthorized access (i.e., command link intrusion)

Category	Essential Threats / Vulnerabilities to Mitigate for Space
	SV-AC-2: Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction
Comms Link	SV-AV-1: Communications system jamming resulting in denial of service and loss of availability and data integrity
	SV-AC-7: Weak communication protocols. Ones that don't have strong support for encryption and authentication within it.
Ground*	SV-MA-7: Exploit ground system and use to maliciously to interact with the spacecraft.
Prevention*	SV-AC-4: Insider Threat not being properly mitigated to prevent malicious interaction or attacking the spacecraft
	SV-SP-4: General supply chain interruption or manipulation. This affects both the hardware and software for both ground and spacecraft
	SV-SP-5: Hardware failure (i.e., tainted hardware). On-board the spacecraft ASICs and FPGAs are heavily used and at due to outsourcing the supply chains that can be compromised.
	SV-SP-10: Compromising the development environment to embed malicious logic or steal trade secrets.
	SV-MA-4: Not planning for security on spacecraft or designing in security from the beginning which is needed to properly build a cyber resilient space system

3.5 Requirement Derivation based on Threats

Using the 5x5 risk matrix analysis, once the risk tolerance is established and the threats/vulnerabilities that require remediation are identified, the program would proceed to requirements generation. Within this document the threats/vulnerabilities listed in the previous figures have already been decomposed into technical requirements and can be leveraged as a starting point for generating the requirements baseline. These technical requirements come in two forms: high-level requirements that provide general terminology to address the threat/vulnerability, and low-level requirements that are the technical level requirements used by system designers. To maintain consistency with existing prescribed policy and control baselines, all the recommended requirements have been cross-referenced to the applicable NIST SP 800-53 and CNSSI 1253 controls. The abbreviation SV is equivalent to space vehicle or spacecraft in the requirement statements. Figure 14 provides representative examples of some high-level requirements that would be gathered based on the results from the notional 5x5 risk analysis previously discussed. You will notice requirement text on the left is cross-referenced to the control tags in the column on the right. The high-level requirement is typically traceable to many underlying controls and supports the rationale for low-level technical requirements derivation. The high-level requirement is typically referenced in higher-level program documentation such as a system specification or a Program Protection Plan (PPP).

High Level Requirement	NIST Controls To Help Mitigate
The SV shall be resilient against communications and positioning jamming attempts.	CP-8,AC-18(5),SC-5,SC-40,SC-40(1),SC-40(3),SI-10,SI-10(3)
The SV shall protect the commanding capability from intrusion.	IA-5(7),SI-10(3),AC-3(10),AU-3(1),IA-5,IA-7,SC-10,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1),SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5), AC-17(1),AC-17(2)
The SV shall prevent previously issued commands from reuse within the systems (i.e. replay attacks).	AU-3(1),IA-2(8),IA-2(9),IA-3,IA-3(1),IA-4,IA-7,SC-13,SC-23,SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5),AC-17(1),AC-17(2)
The Program shall protect the encryption keys from disclosure using a robust key management strategy in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	IA-5,IA-5(7),IA-7,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1)
The Program shall protect against supply chain threats to the SV by employing security safeguards.	CP-2(8),PL-8(2),SA-11(5),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-19,SC-38
The Program shall establish robust procedures and technical methods to prevent the introduction of tainted ASIC and FPGAs into the SV supply chain.	SA-12,SA-12(1)
The Program shall only use acceptable secure communication protocols in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	SA-4(9),SC-8, SC-8(1), SC-8(2), SC-8(3),SI-7(6)
The Program shall specifically develop a defense-in-depth architecture for the SV and document within applicable security documentation.	PL-2, PL-2(3), PL-8, PL-8(1), SA-2, SA-8, SA-17
The Program shall prevent unauthorized access to the SV from the ground segment.	Should have controls from many control families, here are the most important:
The SV shall be resilient against communications and positioning spoofing attempts.	AU-8(1),CP-8,SC-5,SC-40,SC-40(1),SC-40(3),SI-10, SI-10(3)
The SV shall protect communication links from loss in confidentiality.	AC-3(10),SC-7(18),IA-7,SC-13
The Program shall perform software assurance of internally developed and acquired software to include using established robust procedures and technical methods.	CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-3,SA-4(3),SA-4(5),SI-2,SI-2(6),SI-7(14)
The Program shall perform supply chain risk management of all SV software to include using established robust procedures and technical methods.	CA-8,CM-3(2),CM-4(1),CM-5(3),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5)SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-15(7),SA-19,SA-3,SA-4(3),SA-4(5),SC-38,SI-2,SI-7(14)
The SV shall protect mission critical subsystems by ensuring their confidentiality, integrity, and availability are protected during SV operations.	SI-10, SI-10(3),SI-17,CP-12,SC-3
The SV shall employ segregation and least privilege principles for the on-board architecture, communications, and control.	AC-4, AC-4(14), AC-4(2), AC-6, SC-3, SC-4, SC-6, SC-7(21), SC-39, SI-17
The Program shall protect all fault management documents (i.e. FMEA/FMECA artifacts) from inadvertent and inappropriate disclosure.	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SA-5,SC-24,SI-11,SI-17
The SV shall provide the capability to enter the SV into a cyber-safe mode when cyber-attacks have been detected.	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SC-24,SI-11,SI-17
The Program shall ensure all hardware/backdoor commands available for use by the SV are as expected.	SI-10, SI-10(3)
The SV shall recover to normal operations from a cyber-safe mode with executable fault management actions	CP-2(5),IR-4
The SV shall implement protections to prevent components (i.e. payloads) from draining power from the SV.	
The Program shall ensure Software Defined Radios are deemed critical to operations and supply chain risk management strategies are employed for both the hardware and software.	AC-3(2),CA-8,CM-3(2),CM-4(1),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-19,SC-38,SI-2,SI-7(14)
The Program shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.	PM-12

Figure 14: Example Requirements with NIST Controls

Further decomposition from the high-level requirements will be necessary to ensure proper implementation. Using the previously referenced "replay threat," an example decomposition is demonstrated below, and cross referenced to applicable controls tags. In this example the threat/vulnerability rises to a level needing mitigation (rated 23 on the 5x5 risk matrix); therefore, the below requirements would be included in the baseline. This decomposition would repeat for every threat/vulnerability within the list to include any custom additions added through specific mission threat analysis. The full high-to-low decomposition of every threat listed in Figure 13 is available in Appendix A. This full list is being released to aid decisionmakers, acquisition professionals, program managers, and system designers alike with sample requirements for cyber-resilient space systems.

Threat: Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction

- High-Level requirement: The SV shall prevent previously issued commands from reuse within the systems (i.e., replay attacks).

- Low-Level requirements:

  - The SV shall implement relay and replay-resistant authentication mechanisms for establishing a remote connection. {IA-2(8), IA-2(9)}
  - The SV shall uniquely identify and authenticate the ground station and other SVs before establishing a remote connection. {IA-3, IA-4, SI-3(9)}
  - The SV shall authenticate the ground station (and all commands) and other SVs before establishing remote connections using bidirectional authentication that is cryptographically based. {IA-3(1), IA-4, IA-7, SI-3(9), AC-17(2), SC-7(11)}
  - The SV shall fail securely to a secondary device in the event of an operational failure of a primary boundary protection device (i.e., crypto solution). {SC-7(18)}
  - The SV shall restrict the use of information inputs to SVs and designated ground stations as defined in the applicable ICDs. {SC-23, SI-10, SI-10(5)}
  - The SV shall implement cryptography for the indicated uses using the indicated protocols, algorithms, and mechanisms, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: [NSA- certified or approved cryptography for protection of classified information, FIPS-validated cryptography for the provision of hashing] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. {IA-7, SC-13}
  - The SV shall have on-board intrusion detection/prevention system that monitors the mission critical components or systems. {SC-7}
  - The SV shall monitor [Program defined telemetry points] for malicious commanding attempts. {SC-7, AU-3(1), AC-17(1)}

4 Summary

The goal of a threat-based, risk management process is to mitigate cyber risk to below the programs defined risk tolerance threshold. Each program should perform its own detailed analysis to fully understand threats, risks, and countermeasures. By using this approach and defense-in-depth security principles, space cyber risk can be reduced to an acceptable level. Not all risks can be eliminated, and no decisionmaker has unlimited resources to combat all risks but the approach and mitigations discussed herein should help when acquiring, designing, or assessing a cyber-resilient space system.

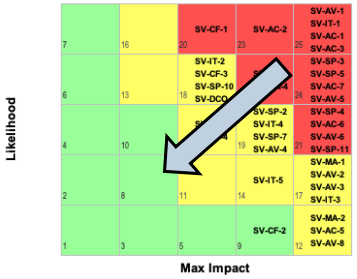


Figure 15: Shifting Cyber Risk to the Left

Given a lack of highly publicized space mission failures attributed to cyberattack, it would be convenient to ignore security. Even though catastrophe has not occurred, China and Russia consider both offensive cyber capabilities and electronic warfare as key assets for maintaining military advantage [22]. This document has also described many examples for maturing space cyber threat capabilities. The protection of space systems is going to be a requirement moving forward as space systems provide critical capabilities for our nation. The release of SPD-5 echoes this same sentiment and articulates the call to arms to address cybersecurity for space across government and commercial sectors. The barrier to entry into space has been drastically reduced and the security by obscurity model is no longer acceptable as the space industry continues significant growth. Defense-in-depth is a substantial part of the solution and cybersecurity needs to be designed in at the beginning of our programs.

For existing systems, the security principles mentioned within this paper can be used as a menu of options available to reduce cyber risk. Not all existing systems will have the ability to deploy new security protection, and some may be limited to primarily improving ground-based security. For future deployments and as cyber protections for space systems mature, the space industry will need to be agile in its verification, validation, and acceptance of risk to keep pace with offensive cyber capabilities. In particular, onboard spacecraft cybersecurity is evolving and will be a challenge as cyber threats continue to mature and system designers will have balance the challenges of size, weight, and power with cybersecurity protection. The government and commercial sectors are beginning to align about the importance of cybersecurity to our space systems; with proper risk management strategies, a combined effort will dramatically improve the cyber health of the space ecosystem.

Appendix A: Threat Informed Requirements Resources

The body of this paper outlined how to perform risk analysis leveraging an example methodology backed by a generic space specific threat model. Other methodologies can be used, but a key aspect is analyzing system design against the predefined list of threats/vulnerabilities. How the ranking is derived is not necessarily important if it accurately reflects the true risk of that particular threat/vulnerability in the mission context. The value proposition of the information in this appendix is that it provides a resource for guidance. Once high-risk threats are identified, the reader may consider or select high-level and low-level technical security requirements for a mission system.

The threats/vulnerabilities have a custom identifier in the form of SV-XX-# which can be used to search/sort the high-level and low-level requirements. The SV stands for Space Vehicle where the XX represents the following:

- AC = Access Control
- IT = Integrity
- AV= Availability
- MA = Mission Assurance
- CF = Confidentiality
- SP = Supply Chain
- DCO = Defensive Cyber Operations

The resources in this appendix are listed in tabular format, but a spreadsheet version of the information makes filtering much easier and is available upon request. However, for the publication of this paper the information was translated to a tabular format.

The first table is the tabular format of Figure 8 with some additional context provided. The following columns are listed in the table.

- ID = Threat/Vulnerability ID
- Threat/Vulnerability Description = Natural language description maintaining as much wording from source material
- Threat/Vulnerability Source = Name of resource where the information was derived from
- CAPEC # = identifier from the CAPEC dictionary of known patterns of attack employed by threat agents/adversaries
- Control Tag Mappings = Identifier/tag from NIST SP 800-53 rev4/CNSSI 1253
- Lowest Threat Tier I-VII to Create Threat Event = Notional representation of which tiered adversary has capability to exploit
- DiD Graphic Subcategory = Category from the Defense-in-Depth graphics (i.e., Figure 6)

Table 5: Threat/Vulnerability Information with Cross References to Various Elements (NIST RMF, Threat Tier, CAPEC, etc.)

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-AC-1	Attempting access to an access-controlled system resulting in unauthorized access	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites * Cybersecurity for Space: Protecting the Final Frontier	20, 21, 94, 102, 114, 115, 161, 180, 248, 463, 594, 616	IA-5(7),SI-10(3),AC-2(11),AC-3(10),AU-3(1),IA-5,IA-7,SC-10,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1),SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5), AC-17(1),AC-17(2),AC-18(1)	III	Crypto
SV-AC-2	Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites	60, 195	AU-3(1),IA-2(8),IA-2(9),IA-3,IA-3(1),IA-4,IA-7,SC-13,SC-23,SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5),AC-17(1),AC-17(2)	III	Crypto
SV-AC-3	Compromised master keys or any encryption key	* CCSDS Threat Green Book * CENTRA Volume I - Cyber Content of Satellites	20, 97, 474, 485,622	IA-5,IA-5(7),IA-7,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1)	III	Data
SV-AC-4	Masquerading as an authorized entity in order to gain access/Insider Threat	* CCSDS Threat Green Book	195, 390, 391, 395, 397, 416	AT-2(2),IR-4(7),PE-3,PM-12, PS-4	IV	Prevention
SV-AC-5	Proximity operations (i.e., grappling satellite)	* CCSDS Threat Green Book	121, 390	SC-41	VI	SBC
SV-AC-6	Three main parts of S/C. CPU, memory, I/O interfaces with parallel and/or serial ports. These are connected via busses (i.e., 1553) and need segregated. Supply chain attack on CPU (FPGA/ASICs), supply chain attack to get malware burned into memory through the development process, and rogue RTs on 1553 bus via hosted payloads are all threats. Security or fault management being disabled by non-mission critical or payload; fault injection or MiTM into the 1553 Bus - China has developed fault injector for 1553 - this could be a hosted payload attack if payload has access to main 1553 bus; One piece of FSW affecting another. Things are not containerized from the OS or FSW perspective;	* CENTRA Volume I - Cyber Content of Satellites * CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards * Orbital Security Alliance - Commercial Space System Security Guidelines	1, 124, 180, 276, 545, 546	AC-4, AC-4(14), AC-4(2), AC-6, SC-3, SC-4, SC-6, SC-7(21), SC-39, SI-17	V	SBC
SV-AC-7	Weak communication protocols. Ones that don't have strong encryption within it	* CENTRA - Cyber Threats to Satellite Networks	192, 272, 276, 277	SA-4(9),SC-8, SC-8(1), SC-8(2), SC-8(3),SI-7(6)	III	Comms Link
SV-AC-8	Malicious Use of hardware commands - backdoors / critical commands	* NASA Mission Resiliency Protection Program Cyber Protection Strategies	88, 248	SI-10, SI-10(3)	III	SBC

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-AV-1	Communications system jamming resulting in denial of service and loss of availability and data integrity	* CCSDS Threat Green Book	559, 599, 603, 619	CP-8,AC-18(5),SC-5,SC-40,SC-40(1),SC-40(3),SI-10,SI-10(3)	V	Comms Link
SV-AV-2	Satellites base many operations on timing especially since many operations are automated. Cyberattack to disrupt timing/timers could affect the vehicle (Time Jamming / Time Spoofing)	* CENTRA Volume I - Cyber Content of Satellites	29, 621, 624		V	SBC
SV-AV-3	Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol	* CENTRA Volume I - Cyber Content of Satellites * Cybersecurity for Space: Protecting the Final Frontier	29, 621, 624		VI	SBC
SV-AV-4	Attacking the scheduling table to affect tasking	* CENTRA Volume I - Cyber Content of Satellites	186, 533	AC-3(2)	V	S/C Software
SV-AV-5	Using fault management system against you. Understanding the fault response could be leveraged to get satellite in vulnerable state. Example, safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of RPO to cause S/C to go into safe mode;	* CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards * Orbital Security Alliance - Commercial Space System Security Guidelines	74, 166, 578, 581, 620	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SA-5,SC-24,SI-11,SI-17	V	IDS/IPS
SV-AV-6	Complete compromise or corruption of running state	* CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards * Orbital Security Alliance - Commercial Space System Security Guidelines	N/A	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SC-24,SI-11,SI-17	V	IDS/IPS
SV-AV-7	The TT&C is the lead contributor to satellite failure over the first 10 years on-orbit, around 20% of the time. The failures due to gyro are around 12% between year one and 6 on-orbit and then ramp up starting around year six and overtake the contributions of the TT&C subsystem to satellite failure. Need to ensure equipment is not counterfeit and the supply chain is sound.	* CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards	520, 522, 530	CP-10,CP-10(4),CP-12,CP-2(8),IR-4,IR-4(3),SA-11(5),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-19,SC-24,SC-3,SC-38,SI-10,SI-10(3),SI-11,SI-17	N/A	Prevention
SV-AV-8	Clock synchronization attack for Spacewire. Since terminals in a distributed system are driven by independent clocks, the clock sync performance is one of the most important indexes in a networked system.	* CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards	624		VI	SBC

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-CF-1	Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determine which entities are communicating with each other without being able to read the communicated information	* CCSDS Threat Green Book	97, 117, 157, 158, 161, 192, 594, 651	AC-3(10),SC-7(18),IA-7,SC-13	III	Crypto
SV-CF-2	Eavesdropping (RF and proximity)	* CCSDS Threat Green Book	117, 619, 623, 651	AC-3(10),IA-7,PE-19,PE-19(1),SC-7(18),SC-13,SC-28,SC-28(1),SI-7(6)	VI	Data
SV-CF-3	Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored Unclass or on contractors' network	* CENTRA Volume I - Cyber Content of Satellites	447, 519, 521	SA-5	III	Prevention
SV-CF-4	Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack	* CENTRA - Chinese Research into Cyber Vulnerabilities of Satellite Bus Standards	20, 97, 117, 158, 620, 621, 622	SC-8, SC-13	V	Crypto
SV-DCO-1	Not knowing that you were attacked, or attack was attempted	* TOR-2018-01164 - Space-Cyber Requirements for Future Systems	N/A	AU-2, AU-3, AU-3(1), AU-4, AU-4(1), AU-5, AU-5(2), AU-6(1), AU-6(4), AU-8, AU-9, AU-9(2),AU-9(3), AU-14, SI-4, SI-4(2), SI-4(4), SI-4(10), SI-4(16), SI-4(5), SI-6, SI-7(8), SI-16, IR-4, IR-5, IR-5(1), SC-5(3), SC-7(9), SI-17, SI-4(11)	V	IDS/IPS
SV-IT-1	Communications system spoofing resulting in denial of service and loss of availability and data integrity	* CCSDS Threat Green Book	148, 151, 627, 628	AU-8(1),CP-8,SC-5,SC-40,SC-40(1),SC-40(3),SI-10, SI-10(3)	V	Crypto
SV-IT-2	Unauthorized modification or corruption of data	* CCSDS Threat Green Book	74, 94, 124, 194, 594	SI-7,SI-7(1),SI-7(2),SI-7(5),SI-7(8),SA-10(1),SC-8,SC-8(2),SC-28,SC-28(1),SI-7(6)	III	Data
SV-IT-3	Compromise boot memory	* CENTRA Volume I - Cyber Content of Satellites	458, 532, 638	SI-7(9)	VI	SBC
SV-IT-4	Cause bit flip on memory via single event upsets	* CENTRA Volume I - Cyber Content of Satellites	No Mapping	SI-16	VI	SBC
SV-IT-5	Onboard control procedures (i.e., ATS/RTS) that execute a scripts/sets of commands	* CENTRA Volume I - Cyber Content of Satellites	186, 533	AC-3(2)	IV	S/C Software
SV-MA-1	Space debris colliding with the SV	* CCSDS Threat Green Book	547		VI	Prevention

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-MA-2	Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyberattacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning	* CCSDS Threat Green Book	622, 623	PE-19,PE-19(1)	VI	Data
SV-MA-3	Attacks on critical software subsystems * Attitude Determination and Control (AD&C) subsystem determines and controls the orientation of the satellite. Any cyberattack that could disrupt some portion of the control loop - sensor data, computation of control commands, and receipt of the commands would impact operations * Telemetry, Tracking and Commanding (TT&C) subsystem provides interface between satellite and ground system. Computations occur within the RF portion of the TT&C subsystem, presenting cyberattack vector * Command and Data Handling (C&DH) subsystem is the brains of the satellite. It interfaces with other subsystems, the payload, and the ground. It receives, validate, decodes, and sends commands to other subsystems, and it receives, processes, formats, and routes data for both the ground and onboard computer. C&DH has the most cyber content and is likely the biggest target for cyberattack. * Electrical Power Subsystem (EPS) provides, stores, distributes, and controls power on the satellite. An attack on EPS could disrupt, damage, or destroy the satellite.	* CENTRA Volume I - Cyber Content of Satellites * Cybersecurity for Space: Protecting the Final Frontier	30, 69	SI-10, SI-10(3),SI-17,CP-12,SC-3	IV	S/C Software
SV-MA-4	Not knowing what your crown jewels are and how to protect them now and in the future.	* Orbital Security Alliance - Commercial Space System Security Guidelines	30, 69	CA-8,CP-2(8),RA-3,SA-12,SA-12(8),SA-14,SA-15(3),SC-7	III	Prevention
SV-MA-5	Not being able to recover from cyberattack	* TOR-2018-01164 - Space-Cyber Requirements for Future Systems	N/A	CP-2(5),IR-4	V	IDS/IPS
SV-MA-6	Not planning for security on SV or designing in security from the beginning	* TOR-2018-02275 - A Need for Robust Space Vehicle Cybersecurity	N/A	PL-2, PL-2(3), PL-8, PL-8(1), SA-2, SA-8, SA-17	I	Prevention

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-MA-7	Exploit ground system and use to maliciously to interact with the SV	* CCSDS Threat Green Book * TOR-2018-02275 - A Need for Robust Space Vehicle Cybersecurity * Cybersecurity for Space: Protecting the Final Frontier	Nearly all CAPECs apply to ground. Analysis indicated 468 out of 524 were applicable to ground. Not listing in this table due to size.	Should have controls from many control families, here are the most important: AC - Access Control AU - Audit and Accountability CM - Configuration Management CP - Contingency Planning IA - Identification and Authentication IR - Incident Response MP - Media Protection PE - Physical and Environmental Protection RA - Risk Assessment CA - Security Assessment and Authorization SC - System and Communications Protection SI - System and Information Integrity SA - System and Services Acquisition	I	Ground

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-MA-8	Payload (or other component) is told to constantly sense or emit or run whatever mission it had to the point that it drained the battery constantly / operated in a loop at maximum power until the battery is depleted.	* Cybersecurity for Space: Protecting the Final Frontier	130		V	SBC
SV-SP-1	Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW.	* CCSDS Threat Green Book	14, 25, 26, 30, 36, 43, 47, 52, 74, 92, 100, 123, 129, 130, 131, 167, 184, 186, 188, 190, 191, 212, 242, 310, 538, 540, 545, 546, 586, 640	CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-3,SA-4(3),SA-4(5),SI-2,SI-2(6),SI-7(14)	II	S/C Software
SV-SP-10	Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3, and SV-SP-4).	* Orbital Security Alliance - Commercial Space System Security Guidelines	443, 444, 511, 537	SA-15	II	Prevention
SV-SP-11	Software defined radios - SDR is also another computer, networked to other parts of the SV that could be pivoted to by an attacker and infected with malicious code. Once access to an SDR is gained, the attacker could alter what the SDR thinks is correct frequencies and settings to communicate with the ground.	* Cybersecurity for Space: Protecting the Final Frontier	184, 186, 401, 440, 442, 443, 445, 446, 452, 511, 516, 520, 522, 523, 531, 534, 535, 537, 583, 624	AC-3(2),CA-8,CM-3(2),CM-4(1),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-19,SC-38,SI-2,SI-7(14)	III	SBC
SV-SP-2	Testing only focuses on functional requirements and rarely considers end to end or abuse cases	* CCSDS Threat Green Book	28, 214, 215, 261	CA-8,RA-5,RA-5(1),RA-5(2),SA-11,SA-11(1),SA-11(2),SA-11(5),SA-11(7),SA-11(8),SA-15(7),SA-3,SA-4(3)	II	Prevention

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-SP-3	Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse	* CCSDS Threat Green Book	68, 185, 186, 187, 206, 441, 442, 443, 444, 445, 446, 456, 511, 523, 533, 552, 640	CA-8,CM-2(2),CM-3(2),CM-4(1),CM-5(3),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5)SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-15(7),SA-19,SA-3,SA-4(3),SA-4(5),SC-38,SI-2,SI-7(14)	III	S/C Software
SV-SP-4	General supply chain interruption or manipulation	* CCSDS Threat Green Book * TOR-2018-02275	438, 441, 444, 544	CP-2(8),PL-8(2),SA-11(5),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-19,SC-38	IV	Prevention
SV-SP-5	Hardware failure (i.e., tainted hardware) {ASIC and FPGA focused}	* CCSDS Threat Green Book	401, 444, 447, 452, 516, 519, 520, 521, 522, 530, 531, 534, 537, 539, 544, 638	SA-12,SA-12(1)	V	Prevention
SV-SP-6	Software reuse, COTS dependence, and standardization of onboard systems using building block approach with addition of open-source technology leads to supply chain threat	* CENTRA Volume I - Cyber Content of Satellites	310, 313, 446, 538	CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SI-2,SI-7(14)	III	S/C Software

ID	Threat/Vulnerability Description	Threat/Vulnerability Source	CAPEC #	Control Tag Mappings	Lowest Threat Tier (I-VII) to Create Threat Event	DiD Graphic Subcategory
SV-SP-7	Software can be broken down into three levels (operating system and drivers' layer, data handling service layer, and the application layer). Highest impact on system is likely the embedded code at the BIOS, kernel/firmware level. Attacking the on-board operating systems. Since it manages all the programs and applications on the computer, it has a critical role in the overall security of the system. Since threats may occur deliberately or due to human error, malicious programs or persons, or existing system vulnerability mitigations must be deployed to protect the OS.	* CENTRA Volume I - Cyber Content of Satellites	186, 312, 313, 532, 638	CA-8,CM-3(2),CM-4(1),CM-7(5),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-4(5),SI-2,SI-7(14)	III	SBC
SV-SP-9	On-orbit software updates/upgrades/patches/direct memory writes. If TT&C is compromised or MOC or even the developer's environment, the risk exists to do a variation of a supply chain attack where after it is in orbit you inject malicious code	* CENTRA - Foreign Satellite Developers, Design, and Cyber Content	186, 187, 445, 533	AC-3(2),CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-3,SA-4(3),SA-4(5),SI-2,SI-2(6),SI-7(14)	III	S/C Software

The below table contains high-level "shall" statements to counteract threats. These are further decomposed into low-level requirements while maintaining traceability and mappings to the SV-XX-# identifiers as well as control tag mappings.

This is also in tabular format with the following columns.

- ID = Threat/Vulnerability ID
- High-Level Requirement = Shall statements to counteract threats
- Control Tag Mappings = Identifier/tag from NIST SP 800-53 rev4/CNSSI 1253
- Notional Risk Rank Score = 1 to 25 ranking using a generic threat model for an example spacecraft mission in low-earth orbit

Table 6: Contains High-level "Shall" Statements to Counteract Threats

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-AC-1	The SV shall protect the commanding capability from intrusion.	IA-5(7),SI-10(3),AC-2(11),AC-3(10),AU-3(1),IA-5,IA-7,SC-10,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1),SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5), AC-17(1),AC-17(2),AC-18(1)	25
SV-AC-2	The SV shall prevent previously issued commands from reuse within the systems (i.e., replay attacks).	AU-3(1),IA-2(8),IA-2(9),IA-3,IA-3(1),IA-4,IA-7,SC-13,SC-23,SC-7,SC-7(11),SC-7(18),SI-3(9),SI-10,SI-10(5),AC-17(1),AC-17(2)	23
SV-AC-3	The Program shall protect the encryption keys from disclosure using a robust key management strategy in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	IA-5,IA-5(7),IA-7,SC-12,SC-12(1),SC-12(2),SC-12(3),SC-13,SC-28(1)	25
SV-AC-4	The Program shall establish policy and procedures to prevent individuals (i.e., insiders) from masquerading as individuals with valid access to areas where commanding of the SV is possible.	AT-2(2),IR-4(7),PE-3,PM-12, PS-4	15
SV-AC-5	The Program shall disable any maintenance and development access to the SV before launch (i.e., JTAG ports)	SC-41	12
SV-AC-6	The SV shall employ segregation and least privilege principles for the on-board architecture, communications, and control.	AC-4, AC-4(14), AC-4(2), AC-6, SC-3, SC-4, SC-6, SC-7(21), SC-39, SI-17	21
SV-AC-7	The Program shall only use acceptable secure communication protocols in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	SA-4(9),SC-8, SC-8(1), SC-8(2), SC-8(3),SI-7(6)	24
SV-AC-8	The Program shall ensure all hardware/backdoor commands available for use by the SV are as expected.	SI-10, SI-10(3)	25
SV-AV-1	The SV shall be resilient against communications and positioning jamming attempts.	CP-8,AC-18(5),SC-5,SC-40,SC-40(1),SC-40(3),SI-10,SI-10(3)	25
SV-AV-2	The SV shall protect the integrity and availability of the authoritative time source.		17
SV-AV-3	The Program shall perform in-depth analysis of watchdog timer implementation to achieve high levels of assurance that the implementation will satisfy mission objections and the availability and integrity is protected.		17
SV-AV-4	The SV shall ensure any update to task scheduling functionality has met high assurance standards before execution.	AC-3(2)	19
SV-AV-5	The Program shall protect all fault management documents (i.e., FMEA/FMECA artifacts) from inadvertent and inappropriate disclosure.	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SA-5,SC-24,SI-11,SI-17	24

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-AV-6	The SV shall provide the capability to enter the SV into a cyber-safe mode when cyberattacks have been detected.	CP-10,CP-10(4),CP-12,IR-4,IR-4(3),SC-24,SI-11,SI-17	21
SV-AV-7	The Program shall apply risk mitigation strategies to reduce the threat of TT&C failing over time.	CP-10,CP-10(4),CP-12,CP-2(8),IR-4,IR-4(3),SA-11(5),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-19,SC-24,SC-3,SC-38,SI-10,SI-10(3),SI-11,SI-17	17
SV-AV-8	The SV shall ensure a robust clock synchronization strategy when Spacewire is utilized on the SV.		12
SV-CF-1	The SV shall protect communication links from loss in confidentiality.	AC-3(10),SC-7(18),IA-7,SC-13	20
SV-CF-2	The SV shall eliminate and then mitigate information leakage due to electromagnetic signals emanations.	AC-3(10),IA-7,PE-19,PE-19(1),SC-7(18),SC-13,SC-28,SC-28(1),SI-7(6)	9
SV-CF-3	The Program shall define and protect Essential Elements of Information (EEI) from unauthorized disclosure.	SA-5	18
SV-CF-4	The SV shall protect the confidentiality and integrity of all information at all times (i.e., transmission, preparation, storage, etc.).	SC-8, SC-13	15
SV-DCO-1	One Liner: The SV shall have intrusion detection, intrusion prevention, and auditing/logging capability on-board the SV that can alert and downlink onboard cyber information to the mission ground station within [mission-appropriate timelines minutes]. Broken Out: The SV shall detect on-board intrusions. The SV shall prevent on-board intrusions. The SV shall audit and log on-board information assurance events. When the SV has detected an intrusion on-board, the SV shall send and alert and onboard cyber information to the mission ground station within [mission-appropriate timelines minutes]. When the SV has prevented an intrusion on-board, the SV shall send and alert and onboard cyber information to the mission ground station within [mission-appropriate timelines minutes].	AU-2, AU-3, AU-3(1), AU-4, AU-4(1), AU-5, AU-5(2), AU-6(1), AU-6(4), AU-8, AU-9, AU-9(2),AU-9(3), AU-14, SI-4, SI-4(2), SI-4(4), SI-4(10), SI-4(16), SI-4(5), SI-6, SI-7(8), SI-16, IR-4, IR-5, IR-5(1), SC-5(3), SC-7(9), SI-17, SI-4(11)	18
SV-IT-1	The SV shall be resilient against communications and positioning spoofing attempts.	AU-8(1),CP-8,SC-5,SC-40,SC-40(1),SC-40(3),SI-10, SI-10(3)	25

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-IT-2	The SV shall protect the confidentiality, integrity, and availability of all information at all times (i.e., transmission, preparation, storage, etc.).	SI-7,SI-7(1),SI-7(2),SI-7(5),SI-7(8),SA-10(1),SC-8,SC-8(2),SC-28,SC-28(1),SI-7(6)	18
SV-IT-3	The SV shall establish a root of trust on the boot process for the flight software.	SI-7(9)	17
SV-IT-4	The SV shall leverage high availability and integrity memory solution to protect from single event upsets.	SI-16	19
SV-IT-5	The SV shall ensure any update to on-board stored procedures has met high assurance standards before execution.	AC-3(2)	14
SV-MA-1	The Program shall mitigate the risk of space debris collision with the SV.		17
SV-MA-2	The SV shall protect mission critical subsystems from electric signal interference.	PE-19,PE-19(1)	12
SV-MA-3	The SV shall protect mission critical subsystems by ensuring their confidentiality, integrity, and availability are protected during SV operations.	SI-10, SI-10(3),SI-17,CP-12,SC-3	25
SV-MA-4	The Program shall ensure all mission critical elements (hardware and software) comply with high levels of assurance for confidentiality, integrity, and availability to meet mission objectives.	CA-8,CP-2(8),RA-3,SA-12,SA-12(8),SA-14,SA-15(3),SC-7	22
SV-MA-5	The SV shall recover to normal operations from a cyber-safe mode with executable fault management actions	CP-2(5),IR-4	24
SV-MA-6	The Program shall specifically develop a defense-in-depth architecture for the SV and document within applicable security documentation.	PL-2, PL-2(3), PL-8, PL-8(1), SA-2, SA-8, SA-17	19

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-MA-7	The Program shall prevent unauthorized access to the SV from the ground segment.	Should have controls from many control families, here are the most important: AC - Access Control AU - Audit and Accountability CM - Configuration Management CP - Contingency Planning IA - Identification and Authentication IR - Incident Response MP - Media Protection PE - Physical and Environmental Protection RA - Risk Assessment CA - Security Assessment and Authorization SC - System and Communications Protection SI - System and Information Integrity SA - System and Services Acquisition	25
SV-MA-8	The SV shall implement protections to prevent components (i.e., payloads) from draining power from the SV.		19
SV-SP-1	The Program shall perform software assurance of internally developed and acquired software using established robust procedures and technical methods.	CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-3,SA-4(3),SA-4(5),SI-2,SI-2(6),SI-7(14)	25
SV-SP-10	The Program shall ensure security requirements/configurations are placed on the development environments to prevent the compromise of source code from supply chain or information leakage perspective.	SA-15	18

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-SP-11	The Program shall ensure Software Defined Radios are deemed critical to operations and supply chain risk management strategies are employed for both the hardware and software.	AC-3(2),CA-8,CM-3(2),CM-4(1),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-19,SC-38,SI-2,SI-7(14)	21
SV-SP-2	The Program shall establish robust procedures and technical methods to perform testing to include negative testing (i.e., abuse cases) of the SV hardware and software.	CA-8,RA-5,RA-5(1),RA-5(2),SA-11,SA-11(1),SA-11(2),SA-11(5),SA-11(7),SA-11(8),SA-15(7),SA-3,SA-4(3)	19
SV-SP-3	The Program shall perform supply chain risk management of all SV software using established robust procedures and technical methods.	CA-8,CM-2(2),CM-3(2),CM-4(1),CM-5(3),CP-2(8),PL-8(2),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5)SA-11(7),SA-11(8),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-15(7),SA-19,SA-3,SA-4(3),SA-4(5),SC-38,SI-2,SI-7(14)	24
SV-SP-4	The Program shall protect against supply chain threats to the SV by employing security safeguards.	CP-2(8),PL-8(2),SA-11(5),SA-12,SA-12(1),SA-12(11),SA-12(2),SA-12(5),SA-12(8),SA-12(9),SA-14,SA-15(3),SA-19,SC-38	21
SV-SP-5	The Program shall establish robust procedures and technical methods to prevent the introduction of tainted ASIC and FPGAs into the SV supply chain.	SA-12,SA-12(1)	24
SV-SP-6	The Program shall ensure reused software meets mission needs and receives or has received adequate software assurance previously.	CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SI-2,SI-7(14)	22

ID	High-Level Requirement	Control Tag Mappings	Notional Risk Rank Score
SV-SP-7	The Program shall ensure SV's operating systems are scrutinized/whitelisted and have received adequate software assurance previously.	CA-8,CM-3(2),CM-4(1),CM-7(5),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-4(5),SI-2,SI-7(14)	19
SV-SP-9	The SV software updates shall be validated for integrity and functionality prior to deployment.	AC-3(2),CA-8,CM-3(2),CM-4(1),CM-5(3),RA-5,RA-5(1),RA-5(2),SA-10,SA-11,SA-11(1),SA-11(2),SA-11(4),SA-11(5),SA-11(6),SA-11(7),SA-11(8),SA-15,SA-15(4),SA-15(5),SA-15(7),SA-15(8),SA-3,SA-4(3),SA-4(5),SI-2,SI-2(6),SI-7(14)	19

Table 7 contains low-level "shall" statements to counteract threats. These are the requirements systems designers would need to design in and account for. The high-level requirements might not be needed, but the low-level requirements are where the real work resides. The entire process of ranking threats/vulnerabilities and identifying risk areas leads to these low-level requirements. The concept if that all the applicable low-level requirements are fully implemented, then the system significantly reduces or mitigates cyber risk. By implementing these low-level requirements, the likelihood of a successful cyberattack is greatly reduced. In some instances, the impact could also be reduced, but that is dependent on the particular threat/vulnerability.

Given the nature of this information, it is presented differently: some low-level requirements address or mitigate multiple threats as well as multiple control tags (i.e., one to many relationships). Therefore, there are only three columns shown. However, on each low-level requirement there are brackets {} that contain the threat/vulnerability ID and the associated control tag.

This is also in tabular format with the following columns.

- Design Considerations or Processes / Procedures = Lists if the requirement is related to a design decision or a procedural augmentation/change
- Low-Level Requirement Text with {Threat ID} {Control Tag}= Shall statements to counteract threats accompanied by a mapping to the threat ID and control tag
- Rationale / Additional Guidance / Notes = Any applicable additional guidance for the requirement.

Table 7: Contains Low-Level "Shall" Statements to Counteract Threats

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall have multiple uplink paths {SV-AV-1} {SC-5,CP-8}	
Design	The SV shall utilize TRANSEC. {SV-AV-1} {CP-8}	Transmission Security (TRANSEC) is used to ensure the availability of transmissions and limit intelligence collection from the transmissions. TRANSEC is secured through burst encoding, frequency hopping, or spread spectrum methods where the required pseudorandom sequence generation is controlled by a cryptographic algorithm and key. Such keys are known as transmission security keys (TSK). The objectives of transmission security are low probability of interception (LPI), low probability of detection (LPD), and antijam which means resistance to jamming (EPM or ECCM).
Design	The SV shall use [directional or beamforming] antennas in normal ops to reduce the likelihood that unintended receivers will be able to intercept signals. {SV-AV-1} {AC-18(5)}	
Design	The SV shall incorporate backup sources for navigation and timing {SV-IT-1}{AU-8(1)}	
Design	The SV shall internally monitor GPS performance so that changes or interruptions in the navigation or timing are flagged. {SV-IT-1} {AU-8(1)}	
Design	The SV shall have fault-tolerant authoritative position and time sourcing. {SV-IT-1} {AU-8(1)}	Adopt voting schemes that include inputs from backup sources. Consider providing a second reference frame against which short-term changes or interferences can be compared.
Design	The SV shall maintain the ability to establish communication with the spacecraft in the event of an anomaly to the primary receive path. {SV-AV-1} {SV-IT-1} {CP-8}	Receiver communication can be established after an anomaly with such capabilities as multiple receive apertures, redundant paths within receivers, redundant receivers, omni apertures, fallback default command modes, and lower bit rates for contingency commanding, as examples
Design	The SV shall protect external and internal communications from jamming and spoofing attempts. {SV-AV-1,SV-IT-1} {SC-5,SC-40,SC-40(1)}	Can be aided via the Crosslink, S-Band, and L-Band subsystems
Design	The SV shall implement cryptographic mechanisms that achieve adequate protection against the effects of intentional electromagnetic interference. {SV-AV-1,SV-IT-1} {SC-40,SC-40(1)}	
Design	The SV shall implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters. {SV-AV-1,SV-IT-1} {SC-40(3)}	
Design	The SV shall implement relay and replay-resistant authentication mechanisms for establishing a remote connection. {SV-AC-1,SV-AC-2} {IA-2(8),IA-2(9)}	
Design	The SV shall uniquely identify and authenticate the ground station and other SVs before establishing a remote connection. {SV-AC-1,SV-AC-2} {IA-3,IA-4,SI-3(9)}	
Design	The SV shall provide the capability to restrict command lock based on geographic location of ground stations. {SV-AC-1} {AC-2(11)}	This could be performed using command lockout based upon when the SV is over selected regions. This should be configurable so that when conflicts arise, the Program can update. The goal is so the SV won't accept a command when the SV determines it is in a certain region.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall authenticate the ground station (and all commands) and other SVs before establishing remote connections using bidirectional authentication that is cryptographically based. {SV-AC-1,SV-AC-2} {IA-3(1),IA-4,IA-7,SI-3(9),AC-17(2),SC-7(11),AC-18(1)}	Authorization can include embedding opcodes in command strings, using trusted authentication protocols, identifying proper link characteristics such as emitter location, expected range of receive power, expected modulation, data rates, communication protocols, beamwidth, etc.; and tracking command counter increments against expected values.
Design	The SV shall not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). {SV-AC-1,SV-CF-1,SV-CF-2} {AC-3(10)}	
Design	The SV shall terminate the connection associated with a communications session at the end of the session or after [TBD minutes] of inactivity. {SV-AC-1} {SC-10}	
Processes / Procedures	The Program shall define policy and procedures to ensure that the developed or delivered systems do not embed unencrypted static authenticators in applications, access scripts, configuration files, nor store unencrypted static authenticators on function keys. {SV-AC-1,SV-AC-3} {IA-5(7)}	
Design	The SV shall protect authenticator content from unauthorized disclosure and modification. {SV-AC-1,SV-AC-3} {IA-5}	
Design	The SV's encryption keys shall be restricted so that they cannot be read via any telecommands. {SV-AC-1,SV-AC-3} {SC-12}	
Design	The SV's encryption keys shall be restricted so that the onboard software is not able to access the information for key readout. {SV-AC-1,SV-AC-3} {SC-12}	
Design	The SV's encryption key handling shall be handled outside of the onboard software and protected using cryptography. {SV-AC-1,SV-AC-3} {SC-12,SC-28(1)}	Examples of devices to handle keys are electron circuits via FPGAs or ASICS. Intent is to ensure the FSW does not have access to crypto keys and system complies with the key management plan.
Design	The SV shall produce, control, and distribute symmetric cryptographic keys using NSA Certified or Approved key management technology and processes. {SV-AC-1,SV-AC-3} {SC-12,SC-12(1),SC-12(2)}	
Design	The Program shall use NIST Approved for symmetric key management for Unclassified systems; NSA Approved or stronger symmetric key management technology for Classified systems. {SV-AC-1,SV-AC-3} {SC-12,SC-12(1),SC-12(2)}	FIPS-complaint technology used by the Program shall include (but is not limited to) cryptographic key generation algorithms or key distribution techniques that are either a) specified in a FIPS, or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS. NSA-approved technology used for symmetric key management by the Program shall include (but is not limited to) NSA-approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria.
Design	The SV shall produce, control, and distribute asymmetric cryptographic keys using [Program-defined] asymmetric key management processes. {SV-AC-1,SV-AC-3} {SC-12,SC-12(1),SC-12(3)}	In most cased the Program will leverage NSA-approved key management technology and processes.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall fail securely to a secondary device in the event of an operational failure of a primary boundary protection device (i.e., crypto solution). {SV-AC-1,SV-AC-2,SV-CF-1,SV-CF-2} {SC-7(18)}	
Design	The SV shall restrict the use of information inputs to SVs and designated ground stations as defined in the applicable ICDs. {SV-AC-1,SV-AC-2} {SC-23,SI-10,SI-10(5)}	
Design	The SV shall implement cryptography for the indicated uses using the indicated protocols, algorithms, and mechanisms, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: [NSA- certified or approved cryptography for protection of classified information, FIPS-validated cryptography for the provision of hashing]. {SV-AC-1,SV-AC-2,SV-CF-1,SV-CF-2,SV-AC-3} {IA-7,SC-13}	
Design	The Program shall use NSA approved key management technology and processes. NSA-approved technology used for asymmetric key management by the Program shall include (but is not limited to) NSA-approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria. {SV-AC-1,SV-AC-3} {SC-12,SC-12(1),SC-12(3)}	
Design	The SV shall have on-board intrusion detection/prevention system that monitors the mission critical components or systems. {SV-AC-1,SV-AC-2,SV-MA-4} {SC-7}	The mission critical components or systems could be GNC/Attitude Control, C&DH, TT&C, Fault Management.
Design	The SV shall monitor [Program defined telemetry points] for malicious commanding attempts. {SV-AC-1,SV-AC-2} {SC-7,AU-3(1),AC-17(1)}	Source from AEROSPACE REPORT NO. TOR-2019-02178 Vehicle Command Counter (VCC) - Counts received valid commands Rejected Command Counter - Counts received invalid commands Command Receiver On/Off Mode - Indicates times command receiver is accepting commands Command Receivers Received Signal Strength - Analog measure of the amount of received RF energy at the receive frequency Command Receiver Lock Modes - Indicates when command receiver has achieved lock on command signal Telemetry Downlink Modes - Indicates when the satellite's telemetry was transmitting Cryptographic Modes - Indicates the operating modes of the various encrypted links Received Commands - Log of all commands received and executed by the satellite System Clock - Master onboard clock GPS Ephemeris - Indicates satellite location derived from GPS Signals
Processes / Procedures	The Program shall have Insider Threat Program to aid in the prevention of people with authorized access to perform malicious activities. {SV-AC-4} {PM-12, AT-2(2),IR-4(7)}	Note: These are not S/C requirements but important to call out but likely are covered under other requirements by the customer.
Design & Processes / Procedures	The Program shall have physical security controls to prevent unauthorized access to the systems that have the ability to command the spacecraft. {SV-AC-4} {PE-3}	
Processes / Procedures	The Program shall have a two-man rule to achieve a high level of security for systems with command level access to the spacecraft. (Under this rule all access and actions require the presence of two authorized people at all times.) {SV-AC-4} {PE-3}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program, upon termination of individual employment, disables information system access within 3 minutes of termination. {SV-AC-4} {PS-4}	
Design & Processes / Procedures	The Program shall require the developer of the system, system component, or system services to demonstrate the use of a system development life cycle that includes [state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes]. {SV-SP-1,SV-SP-2, SV-SP-3,SV-SP-9} {SA-3,SA-4(3)}	Examples of good security practices would be using defense-in-depth tactics across the board, least-privilege being implemented, two factor authentication everywhere possible, using DevSecOps, implementing and validating adherence to secure coding standards, performing static code analysis, component/origin analysis for open source, fuzzing/dynamic analysis with abuse cases, etc.
Processes / Procedures	The Program shall require subcontractors developing information system components or providing information system services (as appropriate) to demonstrate the use of a system development life cycle that includes [state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes]. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-9} {SA-3,SA-4(3)}	Select the particular subcontractors, software vendors, and manufacturers based on the criticality analysis performed for the PPP and the criticality of the components that they supply.
Processes / Procedures	The Program shall require the developer of the system, system component, or system service to deliver the system, component, or service with [Program-defined security configurations] implemented. {SV-SP-1,SV-SP-9} {SA-4(5)}	For the spacecraft FSW, the defined security configuration could include to ensure the software does not contain a pre-defined list of Common Weakness Enumerations (CWEs)and/or CAT I/II Application STIGs.
Processes / Procedures	The Program shall require the developer of the system, system component, or system service to use [Program-defined security configurations] as the default for any subsequent system, component, or service reinstallation or upgrade. {SV-SP-1,SV-SP-3,SV-SP-9} {SA-4(5)}	
Processes / Procedures	The Program shall review proposed changes to the SV, assessing both mission and security impacts. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-10, CM-3(2)}	
Processes / Procedures	The Program shall perform configuration management during system, component, or service during [design; development; implementation; operations]. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-10}	
Processes / Procedures	The Program prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code. {SV-SP-1, SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SI-7(14)}	
Design	The SV shall prevent the installation of Flight Software without verification that the component has been digitally signed using a certificate that is recognized and approved by the Program. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-9} {CM-5(3)}	
Processes / Procedures	The Program shall perform and document threat and vulnerability analyses of the as-built system, system components, or system services. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(2)}	
Processes / Procedures	The Program shall use the threat and vulnerability analyses of the as-built system, system components, or system services to inform and direct subsequent testing/evaluation of the as-built system, component, or service. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(2)}	
Processes / Procedures	The Program shall perform a manual code review of all flight code. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(4)}	
Processes / Procedures	The Program shall conduct an Attack Surface Analysis and reduce attack surfaces to a level that presents a low level of compromise by an attacker. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(6),SA-15(5)}	
Processes / Procedures	The Program shall use threat modeling and vulnerability analysis to inform the current development process using analysis from similar systems, components, or services where applicable. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15(4),SA-15(8)}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall create and implement a security assessment plan that includes: (1) The types of analyses, testing, evaluation, and reviews of [all] software and firmware components; (2) The degree of rigor to be applied to include abuse cases and/or penetration testing; and (3) The types of artifacts produced during those processes. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11,SA-11(5),CA-8}	The security assessment plan should include evaluation of mission objectives in relation to the security of the mission. Assessments should not only be control based but also functional based to ensure mission is resilient against failures of controls.
Processes / Procedures	The Program shall verify that the scope of security testing/evaluation provides complete coverage of required security controls (to include abuse cases and penetration testing) at the depth of testing defined in the test documents. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(5),SA-11(7),CA-8}	* The frequency of testing should be driven by Program completion events and updates. * Examples of approaches are static analyses, dynamic analyses, binary analysis, or a hybrid of the three approaches
Processes / Procedures	The Program shall perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Program-defined depth and coverage]. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11}	The depth needs to include functional testing as well as negative/abuse testing.
Processes / Procedures	The Program shall maintain evidence of the execution of the security assessment plan and the results of the security testing/evaluation. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11,CA-8}	
Processes / Procedures	The Program shall implement a verifiable flaw remediation process into the developmental and operational configuration management process. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11}	The verifiable process should also include a cross reference to mission objectives and impact statements. Understanding the flaws discovered and how they correlate to mission objectives will aid in prioritization.
Processes / Procedures	The Program shall correct flaws identified during security testing/evaluation. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11}	Flaws that impact the mission objectives should be prioritized.
Processes / Procedures	The Program shall perform vulnerability analysis and risk assessment of [all systems and software]. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15(7),RA-5}	
Processes / Procedures	The Program shall identify, report, and coordinate correction of cybersecurity-related information system flaws. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SI-2}	
Processes / Procedures	The Program shall correct reported cybersecurity-related information system flaws, as requested. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SI-2}	* Although this requirement is stated to specifically apply to cybersecurity-related flaws, the Program office may choose to broaden it to all SV flaws. * This requirement is allocated to the Program, as it is presumed, they have the greatest knowledge of the components of the system and when identified flaws apply.
Processes / Procedures	The Program shall test software and firmware updates related to flaw remediation for effectiveness and potential side effects on mission systems in a separate test environment before installation. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SI-2,CM-3(2),CM-4(1)}	This requirement is focused on software and firmware flaws. If hardware flaw remediation is required, refine the requirement to make this clear.
Processes / Procedures	The Program shall release updated versions of the mission information systems incorporating security-relevant software and firmware updates, after suitable regression testing, at a frequency no greater than [Program-defined frequency [90 days]]. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {CM-3(2),CM-4(1)}	On-orbit patching/upgrades may be necessary if vulnerabilities are discovered after launch. The system should have the ability to update software post-launch.
Design	The SV shall be capable of removing flight software after updated versions have been installed. {SV-SP-1,SV-SP-9} {SI-2(6)}	
Processes / Procedures	The Program shall report identified systems or system components containing software affected by recently announced cybersecurity-related software flaws (and potential vulnerabilities resulting from those flaws) to [Program-defined officials] with cybersecurity responsibilities in accordance with organizational policy. {SV-SP-1,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-11} {SI-2}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall ensure that vulnerability scanning tools and techniques are employed that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (1) Enumerating platforms, custom software flaws, and improper configurations; (2) Formatting checklists and test procedures; and (3) Measuring vulnerability impact. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {RA-5}	Component/Origin scanning looks for open-source libraries/software that may be included into the baseline and looks for known vulnerabilities and open-source license violations.
Processes / Procedures	The Program shall create prioritized list of software weakness classes (e.g., Common Weakness Enumerations) to be used during static code analysis for prioritization of static analysis results. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(1),SA-15(7)}	The prioritized list of CWEs should be created considering operational environment, attack surface, etc. Results from the threat modeling and attack surface analysis should be used as inputs into the CWE prioritization process. There is also a CWSS (https://cwe.mitre.org/cwss/cwss_v1.0.1.html) process that can be used to prioritize CWEs. The prioritized list of CWEs can help with tools selection as well as you select tools based on their ability to detect certain high priority CWEs.
Processes / Procedures	The Program shall perform static source code analysis for [all available source code] looking for [Select one {Program-defined Top CWE List, SANS Top 25, OWASP Top 10}] weaknesses using no less than two static code analysis tools. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(1),SA-15(7),RA-5}	
Processes / Procedures	The Program shall perform component analysis (a.k.a. origin analysis) for developed or acquired software. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15(7),RA-5}	
Processes / Procedures	The Program shall analyze vulnerability/weakness scan reports and results from security control assessments. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {RA-5}	
Processes / Procedures	The Program shall determine the vulnerabilities/weaknesses that require remediation, and coordinate the timeline for that remediation, in accordance with the analysis of the vulnerability scan report, the Program assessment of risk, and mission needs. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {RA-5}	
Processes / Procedures	The Program shall share information obtained from the vulnerability scanning process and security control assessments with [Program-defined personnel or roles] to help eliminate similar vulnerabilities in other systems (i.e., systemic weaknesses or deficiencies). {SV-SP-1} {RA-5}	
Processes / Procedures	The Program shall ensure that the vulnerability scanning tools (e.g., static analysis and/or component analysis tools) used include the capability to readily update the list of potential information system vulnerabilities to be scanned. {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {RA-5(1)}	
Processes / Procedures	The Program shall ensure that the list of potential system vulnerabilities scanned is updated [prior to a new scan] {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {RA-5(2)}	
Processes / Procedures	The Program shall define acceptable coding languages to be used by the software developer. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15}	
Processes / Procedures	The Program shall define acceptable secure coding standards for use by the developer. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15}	
Processes / Procedures	The Program shall have automated means to evaluate adherence to coding standards. {SV-SP-1,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-15, SA-15(7),RA-5}	Manual review cannot scale across the code base; you must have a way to scale in order to confirm your coding standards are being met. The intent is for automated means to ensure code adheres to a coding standard.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall employ dynamic analysis (e.g., using simulation, penetration testing, fuzzing, etc.) to identify software/firmware weaknesses and vulnerabilities in developed and incorporated code (open source, commercial, or third-party developed code). {SV-SP-1,SV-SP-2,SV-SP-3,SV-SP-6,SV-SP-7,SV-SP-9,SV-SP-11} {SA-11(5),SA-11(8),CA-8}	Fuzzing and/or dynamic analysis with abuse cases is important to flush out edge cases and how malicious actors could affect the SV's FSW. Not all defects (i.e., buffer overflows, race conditions, and memory leaks) can be discovered statically and require execution of the software. This is where space-centric cyber testbeds (i.e., cyber ranges) are imperative as they provide an environment to maliciously attack components in a controlled environment to discover these undesirable conditions. Technology has improved to where digital twins for spacecraft are achievable, which provides an avenue for cyber testing that was often not performed due to perceived risk to the flight hardware.
Processes / Procedures	The Program shall protect against supply chain threats to the system, system components, or system services by employing [institutional-defined security safeguards] {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12}	The chosen supply chain safeguards should demonstrably support a comprehensive, defense-in-breadth information security strategy. Safeguards should include protections for both hardware and software. Program should define their critical components (HW & SW) and identify the supply chain protections, approach/posture/process.
Processes / Procedures	The Program shall conduct a criticality analysis to identify mission critical functions and critical components and reduce the vulnerability of such functions and components through secure system design. {SV-SP-3,SV-SP-4,SV-AV-7,SV-MA-4} {SA-12,SA-14,SA-15(3),CP-2(8)}	During SCRM, criticality analysis will aid in determining supply chain risk. For mission critical functions/components, extra scrutiny must be applied to ensure supply chain is secured.
Processes / Procedures	The Program shall request threat analysis of suppliers of critical components and manage access to and control of threat analysis products containing U.S. person information. {SV-SP-3,SV-SP-4,SV-SP-11} {SA-12}	The intent of this requirement is to address supply chain concerns on hardware and software vendors. Not required for trusted suppliers accredited to the Defense Microelectronic Activity (DMEA). If the Program intends to use a supplier not accredited by DMEA, the government customer should be notified as soon as possible. If the Program has internal processes to vet suppliers, it may meet this requirement. All software used and its origins must be included in the SBOM and be subjected to internal and Government vulnerability scans.
Processes / Procedures	The Program shall employ the [Program-defined] approaches for the purchase of the system, system components, or system services from suppliers. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(1)}	This could include tailored acquisition strategies, contract tools, and procurement methods.
Design	The SV shall use automated mechanisms to maintain and validate baseline configuration to ensure the SV's is up-to-date, complete, accurate, and readily available. {SV-SP-3} {CM-2(2)}	This could be command trigger from Ground or elsewhere. The point here is that the self-test is executed onboard the SV via onboard HW/SW self-test mechanisms and its result is reported to the Ground

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall maintain documentation tracing the strategies, tools, and methods implemented to the Program-defined strategies, tools, and methods as a means to mitigate supply chain risk . {SV-SP-3,SV-SP-4,SV-AV-7} {SA-12(1)}	Examples include: (1) Transferring a portion of the risk to the developer or supplier through the use of contract language and incentives; (2) Using contract language that requires the implementation of SCRM throughout the system lifecycle in applicable contracts and other acquisition and assistance instruments (grants, cooperative agreements, Cooperative Research and Development Agreements (CRADAs), and other transactions). Within the DOD some examples include: (a) Language outlined in the Defense Acquisition Guidebook section 13.13. Contracting; (b) Language requiring the use of protected mechanisms to deliver elements and data about elements, processes, and delivery mechanisms; (c) Language that articulates that requirements flow down supply chain tiers to sub-prime suppliers. (3) Incentives for suppliers that: (a) Implement required security safeguards and SCRM best practices; (b) Promote transparency into their organizational processes and security practices; (c) Provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; and (d) Implement contract to reduce SC risk down the contract stack. (4) Gaining insight into supplier security practices; (5) Using contract language and incentives to enable more robust risk management later in the lifecycle; (6) Using a centralized intermediary or “Blind Buy” approaches to acquire element(s) to hide actual usage locations from an untrustworthy supplier or adversary;
Processes / Procedures	The Program shall employ [Selection (one or more): independent third-party analysis, Program penetration testing, independent third-party penetration testing] of [Program-defined supply chain elements, processes, and actors] associated with the system, system components, or system services. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(11)}	
Processes / Procedures	The Program shall perform penetration testing/analysis: (1) On potential system elements before accepting the system; (2) As a realistic simulation of the active adversary’s known adversary tactics, techniques, procedures (TTPs), and tools; and (3) Throughout the lifecycle on physical and logical systems, elements, and processes. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-11(5)}	Penetration testing should be performed throughout the lifecycle on physical and logical systems, elements, and processes including: (1) Hardware, software, and firmware development processes; (2) Shipping/handling procedures; (3) Personnel and physical security programs; (4) Configuration management tools/measures to maintain provenance; and (5) Any other programs, processes, or procedures associated with the production/distribution of supply chain elements.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall employ [Program-defined] techniques to limit harm from potential adversaries identifying and targeting the Program supply chain. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(5),SC-38}	Examples of security safeguards that the organization should consider implementing to limit the harm from potential adversaries targeting the organizational supply chain, are: (1) Using trusted physical delivery mechanisms that do not permit access to the element during delivery (ship via a protected carrier, use cleared/official couriers, or a diplomatic pouch); (2) Using trusted electronic delivery of products and services (require downloading from approved, verification-enhanced sites); (3) Avoiding the purchase of custom configurations, where feasible; (4) Using procurement carve outs (i.e., exclusions to commitments or obligations), where feasible; (5) Using defensive design approaches; (6) Employing system OPSEC principles; (7) Employing a diverse set of suppliers; (8) Employing approved vendor lists with standing reputations in industry; (9) Using a centralized intermediary and “Blind Buy” approaches to acquire element(s) to hide actual usage locations from an untrustworthy supplier or adversary Employing inventory management policies and processes; (10) Using flexible agreements during each acquisition and procurement phase so that it is possible to meet emerging needs or requirements to address supply chain risk without requiring complete revision or re-competition of an acquisition or procurement; (11) Using international, national, commercial or government standards to increase potential supply base; (12) Limiting the disclosure of information that can become publicly available; and (13) Minimizing the time between purchase decisions and required delivery.
Processes / Procedures	The Program shall use all-source intelligence analysis of suppliers and potential suppliers of the information system, system components, or system services to inform engineering, acquisition, and risk management decisions. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(8)}	* The Program should also consider sub suppliers and potential sub suppliers. * All-source intelligence of suppliers that the organization may use includes: (1) Defense Intelligence Agency (DIA) Threat Assessment Center (TAC), the enterprise focal point for supplier threat assessments for the DOD acquisition community risks; (2) Other U.S. Government resources including: (a) Government Industry Data Exchange Program (GIDEP) – Database where government and industry can record issues with suppliers, including counterfeits; and (b) System for Award Management (SAM) – Database of companies that are barred from doing business with the US Government.
Processes / Procedures	The Program (and Prime Contractor) shall conduct a supplier review prior to entering into a contractual agreement with a contractor (or sub-contractor) to acquire systems, system components, or system services. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(2)}	
Processes / Procedures	The Program shall maintain a list of suppliers and potential suppliers used, and the products that they supply to include software. {SV-SP-3,SV-SP-4,SV-SP-11} {PL-8(2)}	Ideally you have diversification with suppliers

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall employ [Program-defined Operations Security (OPSEC) safeguards] to protect supply chain-related information for the system, system components, or system services. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-12(9),SC-38,CP-2(8)}	OPSEC safeguards may include: (1) Limiting the disclosure of information needed to design, develop, test, produce, deliver, and support the element for example, supplier identities, supplier processes, potential suppliers, security requirements, design specifications, testing and evaluation result, and system/component configurations, including the use of direct shipping, blind buys, etc.; (2) Extending supply chain awareness, education, and training for suppliers, intermediate users, and end users; (3) Extending the range of OPSEC tactics, techniques, and procedures to potential suppliers, contracted suppliers, or sub-prime contractor tier of suppliers; and (4) Using centralized support and maintenance services to minimize direct interactions between end users and original suppliers.
Processes / Procedures	The Program shall develop and implement anti-counterfeit policy and procedures designed to detect and prevent counterfeit components from entering the information system, including support tamper resistance and provide a level of protection against the introduction of malicious code or hardware. {SV-SP-3,SV-SP-4,SV-AV-7,SV-SP-11} {SA-19}	
Processes / Procedures	The Program shall report counterfeit information system components to [Selection (one or more): source of counterfeit component; [Program-defined external reporting organizations]; [Program-defined personnel or roles]]. {SV-SP-4} {SA-19}	
Processes / Procedures	The Program shall develop and implement anti-counterfeit policy and procedures, in coordination with the [CIO], that is demonstrably consistent with the anti-counterfeit policy defined by the Program office. {SV-SP-4,SV-SP-11} {SA-19}	
Processes / Procedures	The Program shall report counterfeit information system components to the [CIO]. {SV-SP-4} {SA-19}	
Design	The SV shall protect the confidentiality and integrity of all transmitted information. {SV-IT-2} {SC-8}	* The intent as written is for all transmitted traffic to be protected. This includes internal to internal communications and especially outside of the boundary. * Iterate this requirement if different information requires different protection. Refine it, as appropriate, to specific the mechanism to use if that mechanism is not covered by an existing SC-8 enhancement. The Program must assess the strength of mechanisms chosen and determine if they are suitable for mission needs.
Design	The SV shall maintain the confidentiality and integrity of information during preparation for transmission and during reception. {SV-IT-2} {SC-8(2)}	* Preparation for transmission and during reception includes the aggregation, packing, and transformation options performed prior to transmission and the undoing of those operations that occur upon receipt. * As necessary, refine this control to specify the information of interest requiring protection. "
Design	The SV shall protect the confidentiality and integrity of [all information] using cryptography while it is at rest.. {SV-IT-2,SV-CF-2} {SC-28,SC-28(1),SI-7(6)}	* Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. This is often referred to as data-at-rest encryption.
Processes / Procedures	The Program shall define processes and procedures to be followed when the integrity verification tools detect unauthorized changes to [Program-defined software, firmware, and information]. {SV-IT-2} {SI-7}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design & Processes / Procedures	The Program shall enable integrity verification of software and firmware components. {SV-IT-2} {SA-10(1),SI-7}	* The integrity verification mechanisms may include: ** Stipulating and monitoring logical delivery of products and services, requiring downloading from approved, verification-enhanced sites; ** Encrypting elements (software, software patches, etc.) and supply chain process data in transit (motion) and at rest throughout delivery; ** Requiring suppliers to provide their elements "secure by default", so that additional configuration is required to make the element insecure; ** Implementing software designs using programming languages and tools that reduce the likelihood of weaknesses; ** Implementing cryptographic hash verification; and ** Establishing performance and sub-element baseline for the system and system elements to help detect unauthorized tampering/modification during repairs/refurbishing.
Design	The SV shall perform an integrity check of [Program-defined software, firmware, and information] at startup; at [Program-defined transitional states or security-relevant events] {SV-IT-2} {SI-7(1)}	
Design	The Program shall define and document the transitional state or security-relevant events when the SV will perform integrity checks on software, firmware, and information. {SV-IT-2} {SI-7(1)}	
Design	The SV shall provide automatic notification to [Program-defined personnel (e.g., ground operators)] upon discovering discrepancies during integrity verification. {SV-IT-2} {SI-7(2)}	
Design	The Program shall employ automated tools that provide notification to [Program-defined personnel] upon discovering discrepancies during integrity verification. {SV-IT-2} {SI-7(2)}	
Design	The Program shall define the security safeguards that are to be employed when integrity violations are discovered. {SV-IT-2} {SI-7(5)}	
Design	The SV shall automatically [Selection (one or more):restarts the FSW/processor, performs side swap, audits failure; implements Program-defined security safeguards] when integrity violations are discovered. {SV-IT-2} {SI-7(8)}	
Processes / Procedures	Not cyber threat but a generic requirement can be stated The Program shall maintain 24/7 space situational awareness for potential collision with space debris that could come in contact with the SV. {SV-MA-1}	
Design & Processes / Procedures	The Program shall ensure that the contractors/developers have all EEEE, and mechanical piece parts procured from the Original Component Manufacturer (OCM) or their authorized franchised distribution network. {SV-SP-5} {SA-12,SA-12(1)}	These requirements might only make sense for ASIC/FPGA that are deemed to support mission critical functions. The Program has the responsibility to identify all ASICs and FPGAs that are used in all flight hardware by each hardware element. This list must include all contractor and subcontractor usage of ASICs and FPGAs. The Program, working with the contractors, shall identify which ASICs/FPGAs perform or execute an integral part of mission critical functions and if the supplier is accredited "Trusted" by DMEA. If the contractor is not accredited by DMEA, then the Program may apply various of the below ASIC/FPGA assurance requirements to the contractor, and the
Design & Processes / Procedures	Any EEEE or mechanical piece parts that cannot be procured from the OCM or their authorized franchised distribution network shall be approved by the program's Parts, Materials and Processes Control Board (PMPCB) as well as the government program office to prevent and detect counterfeit and fraudulent parts and materials. {SV-SP-5} {SA-12,SA-12(1)}	
Design & Processes / Procedures	The Program shall ensure that the contractors/developers have all ASICs designed, developed, manufactured, packaged, and tested by suppliers with a Defense Microelectronics Activity (DMEA) Trust accreditation. {SV-SP-5} {SA-12,SA-12(1)}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design & Processes / Procedures	For ASICs that are designed, developed, manufactured, packaged, or tested by a supplier that is NOT DMEA accredited Trusted, the ASIC development shall undergo a threat/vulnerability risk assessment. The assessment shall use Aerospace security guidance and requirements tailored from TOR-2019-00506 Vol. 2, and TOR-2019-02543 ASIC and FPGA Risk Assessment Process and Checklist. Based on the results of the risk assessment, the Program may require the developer to implement protective measures or other processes to ensure the integrity of the ASIC. {SV-SP-5} {SA-12,SA-12(1)}	Program may need to perform a risk assessment of the contractor's design environment. DOD-I-5200.44 requires the following: • 4.c.2 "Control the quality, configuration, and security of software, firmware, hardware, and systems throughout their lifecycles... Employ protections that manage risk in the supply chain… (e.g., integrated circuits, field-programmable gate arrays (FPGA), printed circuit boards) when they are identifiable (to the supplier) as having a DOD end-use. " • 4.e "In applicable systems, integrated circuit-related products and services shall be procured from a Trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DOD military end use (generally referred to as application-specific integrated circuits (ASIC)). " • 1.g "In coordination with the DOD CIO, the Director, Defense Intelligence Agency (DIA), and the Heads of the DOD Components, develop a strategy for managing risk in the supply chain for integrated circuit-related products and services (e.g., FPGAs, printed circuit boards) that are identifiable to the supplier as specifically created or modified for DOD (e.g., military temperature range, radiation hardened).
Design & Processes / Procedures	The developer shall use a DMEA certified environment to develop, code and test executable software (firmware or bit-stream) that will be programmed into a one-time programmable FPGA or be programmed into non-volatile memory (NVRAM) that the FPGA executes. {SV-SP-5} {SA-12,SA-12(1)}	
Design & Processes / Procedures	For FPGA pre-silicon artifacts that are developed, coded, and tested by a developer that is NOT DMEA accredited Trusted, the contractor/developer shall be subjected to a development environment and pre-silicon artifacts risk assessment by the Program. The assessment shall use Aerospace security guidance and requirements in TOR-2019-00506 Vol. 2, and TOR-2019-02543 ASIC and FPGA Risk Assessment Process and Checklist. Based on the results of the risk assessment, the Program may require the developer to implement protective measures or other processes to ensure the integrity of the FPGA pre-silicon artifacts. {SV-SP-5} {SA-12,SA-12(1)}	
Processes / Procedures	In the event we want to levy the Government Microelectronics Assessment for Trust (GOMAT) framework outright, to perform ASIC and FPGA threat/vulnerability risk assessment, the following requirements would apply: {SV-SP-5} {SA-12,SA-12(1)} * The GOMAT framework shall be used to perform an initial risk assessment via Aerospace TOR-2019-02543 ASIC/FPGA Risk Assessment Process and Checklist. * The GOMAT framework shall be used to provide ASIC/FPGA lifecycle security guidance and requirements via Aerospace TOR-2019-00506 Volumes & 2 "ASIC and FPGA Lifecyle Security: Threats and Countermeasures". * The GOMAT framework shall be used to perform development environment vulnerability assessment via Aerospace TOR-2019-02543 ASIC/FPGA Risk Assessment Process and Checklist. * The GOMAT framework shall be used to perform development environment vulnerability (DEV) assessment using the tailored DEV requirements from Aerospace TOR-2019-00506 Volume 2. * The GOMAT framework shall be used to perform hardware Trojan horse (HTH) detection independent verification and validation (IV&V). * The GOMAT framework shall be used to perform incremental and final risk assessments via Aerospace TOR-2019-02543 ASIC/FPGA Risk Assessment Process and Checklist. * The GOMAT framework shall be used to recommend mitigations, based on the findings of the risk assessments, to address identified security concerns and vulnerabilities.	
Design	See threat ID SV-AC-for crypto and auth requirements The SV shall be designed such that it protects itself from information leakage due to electromagnetic signals emanations. {SV-CF-2,SV-MA-2} {PE-19,PE-19(1)}	This requirement applies if system components are being designed to address EMSEC and the measures taken to protect against compromising emanations must be in accordance with DODD S-5200.19, or superseding requirements.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall protect system components, associated data communications, and communication buses in accordance with: (i) national emissions and TEMPEST policies and procedures, and (ii) the security category or sensitivity of the transmitted information. {SV-CF-2,SV-MA-2} {PE-19,PE-19(1)}	The measures taken to protect against compromising emanations must be in accordance with DODD S-5200.19, or superseding requirements. The concerns addressed by this control during operation are emanations leakage between multiple payloads within a single space platform, and between payloads and the bus.
Design	The Program shall describe (a) the separation between RED and BLACK cables, (b) the filtering on RED power lines, (c) the grounding criteria for the RED safety grounds, (d) and the approach for dielectric separators on any potential fortuitous conductors. {SV-CF-2,SV-MA-2} {PE-19,PE-19(1)}	
Design	The SV shall provide the capability for data connection ports or input/output devices to be disabled or removed prior to SV operations. {SV-AC-5} {SC-41}	Intent is for external physical data ports to be disabled (logical or physical) while in operational orbit. Port disablement does not necessarily need to be irreversible.
Design	The [software subsystem] shall initialize the SV to a known safe state. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall perform an orderly, controlled system shutdown to a known cyber-safe state upon receipt of a termination command or condition. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall operate securely in off-nominal power conditions, including loss of power and spurious power transients. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall identify and reject commands received out-of-sequence when the out-of-sequence commands can cause a hazard/failure or degrade the control of a hazard or mission. {SV-MA-3,SV-AV-7} {SI-10}	
Design	The [software subsystem] shall detect and recover/transition from detected memory errors to a known cyber-safe state. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall recover to a known cyber-safe state when an anomaly is detected. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall accept [Program defined hazardous] commands only when prerequisite checks are satisfied. {SV-MA-3,SV-AV-7 {SI-10}	
Design	The [software subsystem] shall safely transition between all predefined, known states. {SV-MA-3,SV-AV-7} {SI-17}	The intent of this requirement is to prevent state corruption. Developers should test nominal and off-nominal conditions. It is typically true that some state transitions are not legal by the state transition diagram and are not supported by the design. Legal and illegal state transitions must be tested. Typically the payload(s) are also considered part of this state transition requirement.
Design	The [software subsystem] shall discriminate between valid and invalid input into the software and rejects invalid input. {SV-MA-3,SV-AV-7} {SI-10,SI-10(3)}	
Design	The [software subsystem] shall properly handle spurious input and missing data. {SV-MA-3,SV-AV-7} {SI-10,SI-10(3)}	
Design	The SV shall have failure tolerance on sensors used by software to make mission-critical decisions. {SV-MA-3,SV-AV-7} {SI-17}	
Design	The [software subsystem] shall provide two independent and unique command messages to deactivate a fault tolerant capability for a critical or catastrophic hazard. {SV-MA-3,SV-AV-7} {AC-3(2)}	This requirement was derived from software safety/redundancy standards. The intent is to protect from letting a single command disable the SV or generate a hazard. State transitions, confirmation commands, and other mechanisms could be used to satisfy this control.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The [software subsystem] shall provide at least one independent command for each operator-initiated action used to shut down a function leading to or reducing the control of a hazard. {SV-MA-3,SV-AV-7} {SI-10(5)}	
Design	The [software subsystem] shall provide non-identical methods, or functionally independent methods, for commanding a mission critical function when the software is the sole control of that function. {SV-MA-3,SV-AV-7} {AC-3(2)}	This requirement was derived from software safety/redundancy standards. The intent is to protect from letting a software perform mission critical functions without adequate protection so that if the software fails or is compromised that there are cross checks in place to protection the mission. There should be some secondary control/validation happening when SW is in total control. While autonomy is important and needed, for mission critical functions like thruster burn, SW updates, etc.
Design	The [software subsystem] shall provide independent mission/cyber critical threads such that any one credible event will not corrupt another mission/cyber critical thread. {SV-MA-3,SV-AV-7} {SC-3}	Methods to separate the mission/cyber critical software from software that is not critical, such as partitioning, may be used. If such software methods are used to separate the code and are verified, then the software used in the isolation method is mission/cyber critical, and the rest of the software is not mission/cyber critical. This was derived from software safety/redundancy standards. The intent is to protect from letting a single thread corruption bleed over to corruption of another thread.
Design	The SV's mission/cyber critical commands shall require to be "complex" and/or diverse from other commands so that a single bit flip could not transform a benign command into a hazardous command. {SV-MA-3,SV-AV-7} {SI-10(5)}	
Design	The [software subsystem] shall perform prerequisite checks for the execution of hazardous commands. {SV-MA-3,SV-AV-7} {SI-10}	The intent is to prevent against a single command having a catastrophic system result. E.g., command confirmation could satisfy this control. When designing safety critical systems, single "kill pill" / critical commands must be avoided.
Design	The [software subsystem] shall validate a functionally independent parameter prior to the issuance of any sequence that could remove an inhibit or perform a hazardous action. {SV-MA-3,SV-AV-7} {SI-10(3)}	
Design	The SV shall have fault-tolerant authoritative time sourcing for the SV's clock. {SV-AV-2} {AU-8(2)}	* Adopt voting schemes (triple modular redundancy) that include inputs from backup sources. Consider providing a second reference frame against which short-term changes or interferences can be compared. * Atomic clocks, crystal oscillators and/or GPS receivers are often used as time sources. GPS should not be used as the only source due to spoofing/jamming concerns.
Design	The SV shall synchronize the internal system clocks for each processor to the authoritative time source when the time difference is greater than the FSW-defined interval. {SV-AV-2} {AU-8(1)}	
Design	The [Program-defined security policy] shall state that information should not be allowed to flow between partitioned applications unless explicitly permitted by the Program's security policy. {SV-AC-6} {AC-4}	
Processes / Procedures	The Program shall identify the key system components or capabilities that require isolation through physical or logical means. {SV-AC-6} {SC-3}	Fault management and security management capabilities would be classified as mission critical and likely need separated. Additionally, capabilities like TT&C, C&DH, GNC might need separated as well.
Design	The SV shall enforce approved authorizations for controlling the flow of information within the SV and between interconnected systems based on the [Program defined security policy] that information does not leave the SV boundary unless it is encrypted. {SV-AC-6} {AC-4}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall, when transferring information between different security domains, implements the following security policy filters that require fully enumerated formats that restrict data structure and content: connectors and semaphores implemented in the RTOS. {SV-AC-6} {AC-4(14)}	
Design	The SV shall use protected processing domains to enforce the policy that information does not leave the SV boundary unless it is encrypted as a basis for flow control decisions. {SV-AC-6} {AC-4(2)}	
Design	The SV shall isolate [Program-defined] mission critical functionality from non-mission critical functionality by means of an isolation boundary (implemented via partitions) that controls access to and protects the integrity of, the hardware, software, and firmware that provides that functionality. {SV-AC-6} {SC-3}	* Examine the isolation between mission critical and non-mission critical functionality for each individual information system component. Include architectural considerations in the examination, including isolation derived from using distinct components for mission critical and non-mission critical functionality. This would include having multiple 1553 buses for example to segregate C&DH/TT&C with payload operations. * Methods to separate the mission/cyber critical software from software that is not critical, such as partitioning, may be used (i.e., ARINC 653). If such software methods are used to separate the code and are verified, then the software used in the isolation method is mission/cyber critical, and the rest of the software is not mission/cyber critical. * The intent is to prevent non-mission critical functions/failures from having mission impact. For example some real time operating systems do threading or have the ability to isolate tasks where a failure of one task doesn't affect the SV overall
Design	The SV shall prevent unauthorized access to system resources by employing an efficient capability-based object model that supports both confinement and revocation of these capabilities when the SV security deems it necessary. {SV-AC-6} {SC-4}	
Design	The SV data within partitioned applications shall not be read or modified by other applications/partitions. {SV-AC-6} {SC-4,SC-6}	
Design	The SV shall employ the principle of least privilege, allowing only authorized accesses processes which are necessary to accomplish assigned tasks in accordance with system functions. {SV-AC-6} {AC-6}	
Design	The SV shall maintain a separate execution domain for each executing process. {SV-AC-6} {SC-7(21),SC-39}	
Design	The SV shall implement boundary protections to separate bus, communications, and payload components supporting their respective functions. {SV-AC-6} {SC-7(21)}	
Design	The SV shall ensure that processes reusing a shared system resource (e.g., registers, main memory, secondary storage) do not have access to information (including encrypted representations of information) previously stored in that resource during a prior use by a process after formal release of that resource back to the system or reuse. {SV-AC-6} {SC-4}	
Design	The SV shall prevent unauthorized and unintended information transfer via shared system resources. {SV-AC-6} {SC-4}	
Design	The SV flight software must not be able to tamper with the security policy or its enforcement mechanisms. {SV-AC-6} {SC-3}	
Design	The Program shall define the resources to be allocated to protect the availability of system resources. {SV-AC-6} {SC-6}	
Design	The Program defines the security safeguards to be employed to protect the availability of system resources. {SV-AC-6} {SC-6, SI-17}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV protects the availability of resources by allocating [Program-defined] resources based on [priority and/or quota]. {SV-AC-6} {SC-6}	In particular, this control is required for all space platform buses to ensure execution of high priority functions; it is particularly important when there are multiple payloads sharing a bus providing communications and other services, where bus resources must be prioritized based on mission.
Design	See threat ID number SV-SP-3 for information on software development requirements. In general terms threat ID SV-SP-4 applies from a generic sense since software reuse or COTS usage is a supply chain concern. The Program shall ensure that software planned for reuse meets the fit, form, and function, and security as a component within the new application. {SV-SP-6,SV-SP-7,SV-SP-11} {CM-7(5)}	
Design	The Program shall ensure reused TT&C software has adequate uniqueness for command decoders/dictionaries so that commands are received by only the intended satellite. {SV-SP-6} {SI-3(9)}	The goal is to eliminate risk that compromise of one command database does not affect a different one due to reuse. The intent is to ensure that one SV can not process the commands from another SV. Given the crypto setup with keys and VCC needing to match, this requirement may be inherently met as a result of using type-1 cryptography. The intent is not to recreate entire command dictionaries but have enough uniqueness in place that it prevents a SV from receiving a rogue command. As long as there is some uniqueness at the receiving end of the commands, that is adequate.
Processes / Procedures	This is not a cyber control for the spacecraft, but these controls would apply to ground system, contractor networks, etc. where design sensitive information would reside. NIST 800-17is insufficient to properly protect this information from exposure, exfiltration, etc. Should require contractors to be CMMC 2. 0 Level 3 certified (https://www.acq.osd.mil/cmmc/about-us.html) The Program shall identify and properly classify mission sensitive design/operations information and access control shall be applied in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. {SV-CF-3, SV-AV-5} {SA-5}	* Mission sensitive information should be classified as Controlled Unclassified Information (CUI) or formally known as Sensitive but Unclassified. Ideally these artifacts would be rated SECRET or higher and stored on classified networks. Mission sensitive information can typically include a wide range of candidate material: the functional and performance specifications, the RF ICDs, databases, scripts, simulation and rehearsal results/reports, descriptions of uplink protection including any disabling/bypass features, failure/anomaly resolution, and any other sensitive information related to architecture, software, and flight/ground /mission operations. This could all need protection at the appropriate level (e.g., unclassified, SBU, classified, etc.) to mitigate levels of cyber intrusions that may be conducted against the project's networks. Stand-alone systems and/or separate database encryption may be needed with controlled access and on-going Configuration Management to ensure changes in command procedures and critical database areas are tracked, controlled, and fully tested to avoid loss of science or the entire mission.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall protect documentation and Essential Elements of Information (EEI) as required, in accordance with the risk management strategy. {SV-CF-3, SV-AV-5} {SA-5}	Essential Elements of Information (EEI): **Satellite Description** SCC Number International Designator Name Owner Operator Mission Orbit Slot Orbit Inclination Designer/Builder (Company) Customers (Mil/Gov/Civ) Constellation Description (If Applicable) Status Life Expectancy **Launch Description** Date Country Company Site Vehicle **Radar/Visual Identification Parameters** Radar Cross Section (RCS) Visual Magnitude **Main Bus Description** Make Model Physical Dimensions Structure Design Structure Material Utilized Wet Mass (Beginning-of-Life (BOL)) Dry Mass (End-of-Life (EOL)) Pressurized or Unpressurized Abnormal Features or Appendages Thermal Control System External Material Utilized **Attitude Control System (ACS) Description** Stabilization System Utilized Inertial Measurement Unit (IMU) Gyros (Number) Station-Keeping Primary Control System(s) Station-Keeping Backup Control System(s) Station-Keeping Direction Utilized (Typical) Station-Keeping Frequency Station-Keeping Timeframe Thruster Type Thruster Number Thruster Output Propulsion Type Fuel Type Size of Fuel Container Action Taken After Useful Life (Typical) **Attitude Sensors/Field of View (FOV) Description** Earth Sensor Type Earth Sensor Location on Bus Earth Sensor FOV Horizon Sensor Type Horizon Sensor Location on Bus Horizon Sensor FOV Star Sensor Type Star Sensor Location on Bus Star Sensor FOV Sun Sensor Type Sun Sensor Location on Bus Sun Sensor FOV **Primary Payload Sensor Description** Type Purpose Location of Sensor on Bus FOV **Secondary Payload Sensor** Type Purpose Location of Sensor on Bus FOV **Power System Description** Manufacturer Solar Array Type Solar Array Output Solar Panel Configuration Solar Panel Size Battery Type Battery Number Battery Output Primary Bus Voltage Secondary Bus Voltage **Communication System Description** Antenna Shape Antenna Configuration (Location) **TT&C Frequency/Polarization** Telemetry Signal Type Commanding Signal Type Known Commanding Patterns Known Commanding Periods Beacon Frequency Beacon Polarization **Transponder Description** Transponder Number (Per Band) Transponder Translation Factor (TTF) Transponder Mapping Transponder Power (Amount Used) Transponder Saturation Point Signal of Interest (SOI) (Common Types)
Processes / Procedures	The Program shall distribute documentation to only personnel with defined roles and a need to know. {SV-CF-3,SV-AV-5} {SA-5}	Least privilege and need to know should be employed with the protection of all documentation. Documentation can contain sensitive information that can aid in vulnerability discovery, detection, and exploitation. For example, command dictionaries for ground and space systems should be handles with extreme care. Additionally, design documents for missions contain many key elements that if compromised could aid in an attacker successfully exploiting the system.
Design	Watchdog timers can be implemented via hardware of software. See threat ID SV-SP-3, SV-SP-4, and SV-SP-5 for information on SW, supply chain, and tainted hardware requirements. The watchdog timer is likely considered mission critical/cyber critical therefore requirements from threat ID SV-MA-3 may come into play. Since this threat can be either HW or SW, view the other threat IDs for requirements/controls to mitigate this threat. {SV-AV-3}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall perform attestation at each stage of startup and ensure overall trusted boot regime (i.e., root of trust). {SV-IT-3} {SI-7(9)}	It is important for the computing module to be able to access a set of functions and commands that it trusts; that is, that it knows to be true. This concept is referred to as root of trust (RoT) and should be included in the spacecraft design. With RoT, a device can always be trusted to operate as expected. RoT functions, such as verifying the device's own code and configuration, must be implemented in secure hardware (i.e., field programmable gate arrays). By checking the security of each stage of power-up, RoT devices form the first link in a chain of trust that protects the spacecraft
Design	The trusted boot/RoT shall be a separate compute engine controlling the trusted computing platform cryptographic processor. {SV-IT-3} {SI-7(9)}	
Design	The trusted boot/RoT computing module shall be implemented on radiation tolerant burn-in (non-programmable) equipment. {SV-IT-3} {SI-7(9)}	
Design	The SV boot firmware must verify a trust chain that extends through the hardware root of trust, boot loader, boot configuration file, and operating system image, in that order. {SV-IT-3} {SI-7(9)}	These three items were chosen because they're intended to be static values (once properly set up) but are in volatile storage. Also, the Boot ROM can't be modified, so there's no reason to check a signature.
Design	The SV boot firmware must enter a recovery routine upon failing to verify signed data in the trust chain, and not execute or trust that signed data. {SV-IT-3} {SI-7(9)}	No other requirements are imposed on the recovery routine besides not using the failed data. Unverifiable data isn't trusted and shouldn't be run.
Design	The SV shall allocate enough boot ROM memory for secure boot firmware execution. {SV-IT-3} {SI-7(9)}	
Design	The SV shall allocate enough SRAM memory for secure boot firmware execution. {SV-IT-3} {SI-7(9)}	
Design	The SV secure boot mechanism shall be Commercial National Security Algorithm Suite (CNSA) compliant. {SV-IT-3} {SI-7(9)}	No certification process is required (or exists). The CNSA is easy to meet, only restricts algorithm choice, and aids ease-of-use for government customers.
Design	The SV shall support the algorithmic construct Elliptic Curve Digital Signature Algorithm (ECDSA) NIST P-384 + SHA-38{SV-IT-3} {SI-7(9)}	Timing data may suggest cryptographic accelerators are unnecessary. This construct was chosen because (a) it's in the CNSA suite and (b) it doesn't require secret values to be stored
Design	The SV hardware root of trust must be an ECDSA NIST P-384 public key. {SV-IT-3} {SI-7(9)}	No requirement is imposed on uniqueness.
Design	The SV hardware root of trust must be loadable only once, post-purchase. {SV-IT-3} {SI-7(9)}	No requirement is imposed on preventing hardware readout. The public key belongs to the customer, not the manufacturer, so it must be loaded after purchase. Also, if it can be overwritten, there's no reason to trust it.
Design	The SV boot firmware must validate the boot loader, boot configuration file, and operating system image, in that order, against their respective signatures. {SV-IT-3} {SI-7(9)}	A signature is ~770 bits long. No requirement is imposed on the storage location of signatures.
Design	The SV shall use Error Detection and Correcting (EDAC) memory. {SV-IT-4} {SI-16}	
Design	The SV shall utilize an EDAC scheme to routinely check for bit errors in the stored data on board the spacecraft, correct the single-bit errors, and identify the memory addresses of data with uncorrectable multi-bit errors of at least order two, if not higher order in some cases. {SV-IT-4} {SI-16}	
Design	The SV shall integrate EDAC scheme with fault management and cyber-protection mechanisms to respond to the detection of uncorrectable multi-bit errors, other than time-delayed monitoring of EDAC telemetry by the mission operators on the ground. {SV-IT-4} {SI-16}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV's fault management solution shall utilize memory uncorrectable bit error detection information in a strategy to autonomously minimize the adverse effects of uncorrectable bit errors within the spacecraft. {SV-IT-4} {SI-16}	
Design	The SV's Interrupt Service Routine (ISR) shall have the ability to simultaneously update check-bits for [Program-defined] memory addresses. {SV-IT-4} {SI-16}	
Processes / Procedures	The Program shall perform static binary analysis of all firmware that is utilized on the spacecraft. {SV-SP-7,SV-SP-11} {SA-11,RA-5}	Many commercial products/parts are utilized within the system and should be analyzed for security weaknesses. Blindly accepting the firmware is free of weakness is unacceptable for high assurance missions. The intent is to not blindly accept firmware from unknown sources and assume it is secure. This is meant to apply to firmware the vendors are not developing internally. In-house developed firmware should be going through the vendor's own testing program and have high assurance it is secure. When utilizing firmware from other sources, "expecting" does not meet this requirement. Each supplier needs to provide evidence to support that claim that their firmware they are getting is genuine and secure.
Processes / Procedures	The Program shall define/maintain an approved operating system list for use on spacecraft. {SV-SP-7} {CM-7(5)}	The operating system is extremely important to security and availability of the spacecraft, therefore should receive high levels of assurance that it operates as intended and free of critical weaknesses/vulnerabilities.
Design	The SV's operating system, if COTS or FOSS, shall be selected from a [Program-defined] accepted list. {SV-SP-7} {SI-7(14),CM-7(5)}	
Design	The SV shall retain the capability to update/upgrade operating systems while on-orbit. {SV-SP-7} {SA-4(5)}	The operating system updates should be performed using multi-factor authorization and should only be performed when risk of compromise/exploitation of identified vulnerability outweighs the risk of not performing the update.
Design	The SV shall require multi-factor authorization for all updates to the task scheduling functionality within the spacecraft. {SV-AV-4} {AC-3(2)}	Multi-factor authorization could be the "two-man rule" where procedures are in place to prevent a successful attack by a single actor (note: development activities that are subsequently subject to review or verification activities may already require collaborating attackers such that a "two-man rule" is not appropriate).
Design	The SV shall require multi-factor authorization for new and updates to on-board stored command sequences. {SV-IT-5} {AC-3(2)}	Multi-factor authorization could be the "two-man rule" where procedures are in place to prevent a successful attack by a single actor (note: development activities that are subsequently subject to review or verification activities may already require collaborating attackers such that a "two-man rule" is not appropriate).
Design	The Program shall define acceptable secure communication protocols available for use within the mission in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. {SV-AC-7} {SA-4(9)}	The secure communication protocol should include "strong" authenticated encryption characteristics.
Design	The SV shall only use [Program-defined] communication protocols within the mission. {SV-AC-7} {SA-4(9)}	
Design	The SV shall protect the confidentiality and integrity of the [all] transmitted information. {SV-AC-7} {SC-8}	
Design	The SV shall implement cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission unless otherwise protected by alternative physical safeguards. {SV-AC-7} {SC-8(1),SI-7(6)}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall maintain the confidentiality and integrity of information during preparation for transmission and during reception. {SV-AC-7} {SC-8(2)}	
Design	The SV shall implement cryptographic mechanisms to protect message externals unless otherwise protected by alternative physical safeguards. {SV-AC-7} {SC-8(3)}	
Design	See threat ID SV-CF-3 to help with protecting design specific information, in this case the FMEA/FMECA artifacts so that particular fault responses are not disclosed via documentation. {SV-AV-5}	
Design	The SV shall provide or support the capability for recovery and reconstitution to a known state after a disruption, compromise, or failure. {SV-AV-5,SV-AV-6,SV-AV-7} {CP-10,CP-10(4),IR-4}	
Design	The SV shall provide the capability to enter the SV into a configuration-controlled and integrity-protected state representing a known, operational cyber-safe state (e.g., cyber-safe mode). {SV-AV-5,SV-AV-6,SV-AV-7} {CP-12,SI-17,IR-4(3)}	Cyber-safe mode is an operating mode of a spacecraft during which all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. Within cyber-safe mode authentication and encryption should still be enabled. The spacecraft should be capable of reconstituting firmware and SW functions to preattack levels to allow for the recovery of functional capabilities. This can be performed by self-healing, or the healing can be aided from the ground. However, the spacecraft needs to have the capability to replan, based on available equipment still available after a cyberattack. The goal is for the vehicle to resume full mission operations. If not possible, a reduced level of mission capability should be achieved.
Design	The SV shall enter a cyber-safe mode when conditions that threaten the SV are detected with restrictions as defined based on the cyber-safe mode. {SV-AV-5,SV-AV-6,SV-AV-7} {CP-12,SI-17,IR-4(3)}	
Design	The SV's cyber-safe mode software/configuration should be stored onboard the spacecraft in memory with hardware-based controls and should not be modifiable. {SV-AV-5,SV-AV-6,SV-AV-7} {SI-17}	Cyber-safe mode is using a fail-secure mentality where if there is a malfunction that the SV goes into a fail-secure state where cyber protections like authentication and encryption are still employed (instead of bypassed) and the SV can be restored by authorized commands. The cyber-safe mode should be stored in a high integrity location of the on-board SV so that it cannot be modified by attackers.
Design	The SV shall fail to a known secure state for all types of failures preserving information necessary to determine cause of failure and to return to operations with least disruption to mission operations. {SV-AV-5,SV-AV-6,SV-AV-7} {SC-24,SI-17}	
Design	The SV shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. {SV-AV-5,SV-AV-6,SV-AV-7} {SI-11}	
Design	The SV shall reveal error messages only to operations personnel monitoring the telemetry. {SV-AV-5,SV-AV-6,SV-AV-7} {SI-11}	
Design	Nothing specific to eliminate the availability threat of TT&C failing over time. Requirements are covered under threat ID SV-SP-3, SV-SP-4,SV-MA-3 and SV-AV-Strong fault management and redundancy also helps mitigate threats against TT&C. {SV-AV-7}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	If Spacewire is utilized, then the SV shall adhere to [Program-defined] time synchronization standard/protocol to synchronize time across a Spacewire network with an accuracy around 1 microsecond. {SV-AV-8} {AU-8(1)}	Example for time synchronization is Time Distribution Protocol (http://spacewire.esa.int/WG/Spacewire/SpW-WG-Mtg17-Proceedings/Documents/ISC_2011%20CCSDS%20Time%20Distribution%20over%20SpaceWire.pdf & https://amstel.estec.esa.int/tecedm/ipcores/time_sync_protocol.pdf). These activities by ESA are looking to perform standardization of a time distribution protocol, synchronization, and handling of latency, jitter, and drift
Design	The spacecraft cannot cloak that it is in a sun pointing mode, but the downlinked information should still be encrypted so that it cannot be received by unauthorized adversary. The SV shall encrypt all telemetry on downlink regardless of operating mode to protect current state of spacecraft. {SV-CF-4} {SC-8,SC-13}	
Design	See threat ID number SV-SP-SW update and supply chain protections. But any SW update should have two-man rule like in threat ID SV-AV-4 and SV-IT-6. The SV shall require multi-factor authorization for all SV [applications or operating systems] updates within the spacecraft. {SV-SP-9,SV-SP-11} {AC-3(2)}	The intent is for multiple checks to be performed prior to executing these SV SW updates. One action is mere act of uploading the SW to the SV. Another action could be check of digital signature (ideal but not explicitly required) or hash or CRC or a checksum. Crypto boxes provide another level of authentication for all commands, including SW updates but ideally there is another factor outside of crypto to protect against FSW updates.
Processes / Procedures	The Program shall use all-source intelligence analysis on threats to mission critical capabilities and/or system components to inform risk management decisions. {SV-MA-4} {SA-12(8)}	
Processes / Procedures	The Program shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the SV and the information it processes, stores, or transmits. {SV-MA-4} {RA-3}	Risk assessment is an iterative process. The first assessment occurs early in the process to assess the base design, select mitigating and program specific controls. Assessments continue as the design development continues in order to assess and mitigate new risks and/or threats. This continues throughout the lifecycle because new risks/threats can develop from new vulnerabilities.
Processes / Procedures	The Program's risk assessment shall include the full end to end communication pathway from the ground to the spacecraft. {SV-MA-4} {RA-3}	
Processes / Procedures	The Program shall document risk assessment results in [risk assessment report]. {SV-MA-4} {RA-3}	
Processes / Procedures	The Program shall review risk assessment results [At least annually if not otherwise defined in formal organizational policy]. {SV-MA-4} {RA-3}	
Processes / Procedures	The Program shall update the risk assessment [At least annually if not otherwise defined in formal institutional policy] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the SV. {SV-MA-4} {RA-3}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Processes / Procedures	The Program shall coordinate penetration testing on [program-defined mission critical SV components (hardware and/or software)]. {SV-MA-4} {CA-8}	Not all defects (i.e., buffer overflows, race conditions, and memory leaks) can be discovered statically and require execution of the system. This is where space-centric cyber testbeds (i.e., cyber ranges) are imperative as they provide an environment to maliciously attack components in a controlled environment to discover these undesirable conditions. Technology has improved to where digital twins for spacecraft are achievable, which provides an avenue for cyber testing that was often not performed due to perceived risk to the flight hardware.
Design & Processes / Procedures	This is not a cyber control for the spacecraft, but these controls would apply to ground system, contractor networks, etc. where design sensitive information would reside. NIST 800-17is insufficient to properly protect this information from exposure, exfiltration, etc. See threat ID SV-SP-1, SV-SP-3, and SV-SP-4 for information on secure SW and supply chain protection. Should require contractors to be CMMC 2.0 Level 3 certified (https://www.acq.osd.mil/cmmc/about-us.html) The Program shall ensure [Program defined] security requirements/configurations are placed on the development environments to prevent the compromise of source code from supply chain or information leakage perspective. {SV-SP-10} {SA-15}	Source code should be classified as Controlled Unclassified Information (CUI) or formally known as Sensitive but Unclassified. Ideally source code would be rated SECRET or higher and stored on classified networks. NIST 800-171 is insufficient when protecting highly sensitive unclassified information and more robust controls from NIST SP 800-53 and CNSSI 1253 should be employed. Greater scrutiny must be applied to all development environments.
Design	The Program shall perform analysis of critical (backdoor) commands that could adversely affect mission success if used maliciously. {SV-AC-8} {SI-10,SI-10(3)}	Heritage and commercial products often have many residual operational (e.g., hardware commands) and test capabilities that are unidentified or unknown to the end user, perhaps because they were not expressly stated mission requirements. These would never be tested and their effects unknown, and hence, could be used maliciously. Test commands not needed for flight should be deleted from the flight database.
Design	The Program shall ensure that all viable commands are known to the mission and SV "owner. {SV-AC-8} {SI-10,SI-10(3)}	This is a concern for bus re-use. It is possible that the manufacturer left previously coded commands in their syntax rather than starting from a clean slate. This leaves potential backdoors and other functionality the mission does not know about.
Design	The SV shall only use or include [Program-defined] critical commands for the purpose of providing emergency access where commanding authority is appropriately restricted. {SV-AC-8} {SI-10,SI-10(3)}	The intent is protect against misuse of critical commands. On potential scenario is where you could use accounts with different privileges, could require an additional passphrase or require entry into a different state or append an additional footer to a critical command. There is room for design flexibility here that can still satisfy this requirement.

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall monitor and collect all onboard cyber-relevant data (from multiple system components), including identification of potential attacks and sufficient information about the attack for subsequent analysis. {SV-DCO-1} {SI-4,SI-4(2),AU-2}	The spacecraft will monitor and collect data that provides accountability of activity occurring onboard the spacecraft. Due to resource limitations on the spacecraft, analysis must be performed to determine which data is critical for retention and which can be filtered. Full system coverage of data and actions is desired as an objective; it will likely be impractical due to the resource limitations. “Cyber-relevant data” refers to all data and actions deemed necessary to support accountability and awareness of onboard cyber activities for the mission. This would include data that may indicate abnormal activities, critical configuration parameters, transmissions on onboard networks, command logging, or other such data items. This set of data items should be identified early in the system requirements and design phase. Cyber-relevant data should support the ability to assess whether abnormal events are unintended anomalies or actual cyber threats. Actual cyber threats may rarely or never occur, but non-threat anomalies occur regularly. The ability to filter out cyber threats for non-cyber threats in relevant time would provide a needed capability. Examples could include successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels).
Design	The SV shall generate cyber-relevant audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, and the outcome of the event. {SV-DCO-1} {AU-3, AU-3(1)}	
Design	The SV shall use internal system clocks to generate time stamps for audit records. {SV-DCO-1} {AU-8}	
Design	The SV shall record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). {SV-DCO-1} {AU-8}	
Design	The SV shall record time stamps for audit records that provide a granularity of one Z-count (1.5 sec). {SV-DCO-1} {AU-8}	
Design	The SV shall be designed and configured so that [Program-defined encrypted communications traffic and data] is visible to on-board monitoring tools. {SV-DCO-1} {SI-4(10)}	
Design	The SV shall be designed and configured so that SV memory can be monitored by the on-board intrusion detection/prevention capability. {SV-DCO-1} {SI-16}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall provide automated onboard mechanisms that integrate audit review, analysis, and reporting processes to support mission processes for investigation and response to suspicious activities to determine the attack class in the event of a cyberattack. {SV-DCO-1} {SC-5(3),AU-6(1)}	* Identifying the class (e.g., exfiltration, Trojans, etc.), nature, or effect of cyberattack (e.g., exfiltration, subverted control, or mission interruption) is necessary to determine the type of response. The first order of identification may be to determine whether the event is an attack or a non-threat event (anomaly). The objective requirement would be to predict the impact of the detected signature. * Unexpected conditions can include RF lockups, loss of lock, failure to acquire an expected contact and unexpected reports of acquisition, unusual AGC and ACS control excursions, unforeseen actuator enabling's or actions, thermal stresses, power aberrations, failure to authenticate, software or counter resets, etc. Mitigation might include additional TMONs, more detailed AGC and PLL thresholds to alert operators, auto-capturing state snapshot images in memory when unexpected conditions occur, signal spectra measurements, and expanded default diagnostic telemetry modes to help in identifying and resolving anomalous conditions.
Design	The SV shall integrate cyber related detection and responses with existing fault management capabilities to ensure tight integration between traditional fault management and cyber intrusion detection and prevention. {SV-DCO-1} {AU-6(4),SI-4(16)}	The onboard IPS system should be integrated into the existing onboard spacecraft fault management system (FMS) because the FMS has its own fault detection and response system built in. SV corrective behavior is usually limited to automated fault responses and ground commanded recovery actions. Intrusion prevention and response methods will inform resilient cybersecurity design. These methods enable detected threat activity to trigger defensive responses and resilient SV recovery.
Design	The SV shall be able to locate the onboard origin of a cyberattack and alert ground operators within [TBD minutes]. {SV-DCO-1} {SI-4(16)}	The origin of any attack onboard the vehicle should be identifiable to support mitigation. At the very least, attacks from critical element (safety-critical or higher-attack surface) components should be locatable quickly so that timely action can occur.
Design	The SV shall attribute cyberattacks and identify unauthorized use of the SV by downlinking onboard cyber information to the mission ground station within [mission-appropriate timelines minutes]. {SV-DCO-1} {AU-4(1), SI-4(5)}	Requirement is to support offboard attribution by enabling the fusion of spacecraft cyber data with ground-based cyber data. This would provide end-to-end accountability of commands, data, and other data that can be used to determine the origin of attack from the ground system. Data should be provided within time constraints relevant for the particular mission and its given operational mode. Analysis should be performed to identify the specific timeliness requirements for a mission, which may vary depending on mission mode, operational status, availability of communications resources, and other factors. The specific data required should be identified, as well.
Design	The SV shall detect and deny unauthorized outgoing communications posing a threat to the SV. {SV-DCO-1} {SI-4(4),SC-7(9),SI-4(11)}	
Design	The SV shall protect information obtained from logging/intrusion-monitoring from unauthorized access, modification, and deletion. {SV-DCO-1} {AU-9}	
Design	The SV shall implement cryptographic mechanisms to protect the integrity of audit information and audit tools. {SV-DCO-1} {AU-9(3)}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall select and execute safe countermeasures against cyberattacks prior to entering cyber-safe mode. {SV-DCO-1} {SI-17,IR-4}	These countermeasures are a ready supply of options to triage against the specific types of attack and mission priorities. Minimally, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker exquisitely—with or without ground aiding. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. “Safe countermeasures” are those that are compatible with the system’s fault management system to avoid unintended effects or fratricide on the system." These countermeasures are likely executed prior to entering into a cyber-safe mode.
Design	The SV shall provide cyber threat status to the ground segment for the Defensive Cyber Operations team, per the governing specification. {SV-DCO-1} {IR-5}	The future space enterprises will include full-time Cyber Defense teams supporting space mission systems. Their work is currently focused on the ground segment but may eventually require specific data from the space segment for their successful operation. This requirement is a placeholder to ensure that any DCO-related requirements are taken into consideration for this document.
Design	The SV shall provide an alert immediately to [at a minimum the mission director, administrators, and security officers] when the following failure events occur: [minimally but not limited to auditing software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity reaching 95%, 99%, and 100%] of allocated capacity. {SV-DCO-1} {AU-5(2)}	Intent is to have human on the ground be alerted to failures. This can be decomposed to SV to generate telemetry and to Ground to alert.
Design	The SV shall provide the capability of a cyber “black-box” to capture [Program-defined information] necessary data for cyber forensics of threat signatures and anomaly resolution when cyberattacks are detected. {SV-DCO-1} {IR-5(1),AU-9(2)}	Similar concept of a "black box" on an aircraft where all critical information is stored for post forensic analysis. Black box can be used to record CPU utilization, GNC physical parameters, audit records, memory contents, TT&C data points, etc. The timeframe is dependent upon implementation but needs to meet the intent of the requirement. For example, 30 days may suffice.
Design	The SV shall alert in the event of the [Program-defined] audit/logging processing failures. {SV-DCO-1} {AU-5}	
Design	The SV shall provide the capability to verify the correct operation of security-relevant software and hardware mechanisms (e.g., SV IDS/IPS, logging, crypto, etc.) {SV-DCO-1} {SI-6}	
Design	The SV, upon detection of a potential integrity violation, shall provide the capability to [audit the event and alert ground operators]. {SV-DCO-1} {SI-7(8)}	One example would be for bad commands where the system would reject the command and not increment the Vehicle Command Counter (VCC) and include the information in telemetry.
Design	The SV shall be configured to allocate audit record storage capacity in accordance with [Program-defined audit record storage requirements]. {SV-DCO-1} {AU-4}	
Design	The SV shall provide the capability to modify the set of audited events (e.g., cyber-relevant data). {SV-DCO-1} {AU-14}	
Design	The Program shall integrate terrestrial system audit log analysis as part of the standard anomaly resolution process to correlate any anomalous behavior in the terrestrial systems that correspond to anomalous behavior in the SV. {SV-DCO-1} {AU-6(1), IR-5(1)}	

Design Considerations or Processes / Procedures	Low-Level Requirement Text with {Threat ID} {Control Tag}	Rationale / Additional Guidance / Notes
Design	The SV shall recover from cyber-safe mode to mission operations within [mission-appropriate timelines 5 minutes]. {SV-MA-5} {CP-2(5), IR-4}	Upon conclusion of addressing the threat, the system should be capable of recovering from the minimal survival mode back into a mission-ready state within defined timelines. The intent is to define the timelines and the capability to return back to mission operations.
Processes / Procedures	The Program shall develop a security plan for the SV. {SV-MA-6} {PL-2}	
Processes / Procedures	The Program shall protect the security plan from unauthorized disclosure and modification. {SV-MA-6} {PL-2}	
Processes / Procedures	The Program shall plan and coordinate security-related activities affecting the SV with groups associated with systems from which the SV is inheriting satisfaction of controls before conducting such activities in order to reduce the impact on other organizational entities. {SV-MA-6} {PL-2(3)}	
Design	The Program shall document and design a security architecture using a defense-in-depth approach that allocates the Program defined safeguards to the indicated locations and layers: [Examples include operating system abstractions and hardware mechanisms to the separate processors in the SV, internal components, and the FSW]. {SV-MA-6} {PL-8,PL-8(1)}	
Design	The Program shall ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner. {SV-MA-6} {PL-8(1)}	
Design	The Program shall implement a security architecture and design that provides the required security functionality, allocates security controls among physical and logical components, and integrates individual security functions, mechanisms, and processes together to provide required security capabilities and a unified approach to protection. {SV-MA-6} {SA-2,SA-8}	
Processes / Procedures	The Program shall document the SV's security architecture, and how it is established within and is an integrated part of the Program's mission security architecture. {SV-MA-6} {SA-17}	
Design & Processes / Procedures	Ground should have requirements/controls around: Data Protection, Ground Software, Endpoints, Networks, Computer Network Defense / Incident Response, Perimeter Security, Physical Controls, and Prevention Program (SSP, PPP, and Training). See NIST 800-53 and CNSSI 1253 for guidance on ground security {SV-MA-7}	
Design & Processes / Procedures	This would be similar to inserting malicious logic into the SV during the development (HW and SW supply chain which are covered under SV-SP-5, SV-SP-3, and SV-SP-4)or via SW update process once launched which is covered under threat ID SV-SP-9. Depending on the implementation of the payload/component the controls would be different therefore specific requirements are not generated for this particular threat but are covered by other threats. Additionally, EPS related requirements/controls were also mentioned with SV-MA-3 {SV-MA-8}	
Design & Processes / Procedures	This would be similar to inserting malicious logic into the SV during the development (HW and SW supply chain which are covered under SV-SP-3, SV-SP-4, SV-SP-6, and SV-SP-7)or via SW update process once launched which is covered under threat ID SV-SP-9. Depending on the implementation of the SDR the controls would be different therefore specific requirements are not generated for this particular threat but are covered by other threats. {SV-SP-11}	

Appendix B: References

[1] White House; *Space Policy Directive – 5*, September 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

[2] Defense Intelligence Agency; *Challenges to Security in Space,* February 11, 2019, pages 9, 20, 29, and 36, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[3] Weeden, B; Samson, V; *Global Counterspace Capabilities: An Open Source Assessment,* April 2018, page 7-1, https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[4] Lucian Kim; *U.S. Slaps New Sanctions On Russia Over Cyberattack, Election Meddling*, https://www.npr.org/2021/04/15/987585796/u-s-slaps-new-sanctions-on-russia-over-cyber-attack-election-meddling

[5] Porup, J; "It's Surprisingly Simple to Hack a Satellite", August 21, 2015, https://www.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

[6] Eddy, M; "Satellite Communications Hacks Are Real, and They're Terrifying", August 9, 2018, https://www.pcmag.com/news/363004/satellite-communications-hacks-are-real-and-theyre-terrify.

[7] James Pavur, Dphil Student, *Whispers Among the Stars: Perpetrating (and Preventing) Satellite Eavesdropping Attacks,* August 2020, BlackHat USA 2020

[8] Ewart, R; Wheler, W; Betser, J; Cohen, N; Knobbe, R; Horejsi, J; Gonce, J; *Cyber Enhanced Space Operations from Frameworks to Enterprise Evolution,* September 2016, https://arc.aiaa.org/doi/pdf/10.2514/6.2016-5474

[9] Bailey, B; Wheler, W; Doshi, P; Cohen, N; Speelman, R; *Defending Spacecraft in the Cyber Domain,* November 2019, https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

[10] Livingston, D; Lewis, P; *Space, the Final Frontier for Cybersecurity?,* September 2016, page 21, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[11] Orly Stan, Yuval Elovici, Asaf Shabtai, Gaby Shugol, Raz Tikochinski, Shachar Kur; *Protecting Military Avionics Platforms from Attacks on MIL-STD-1553 Communication Bus,* July 2017, https://arxiv.org/pdf/1707.05032.pdf

[12] Ginter, A; "The Top 20 Cyberattacks on Industrial Control Systems," January 25, 2018, https://waterfall-security.com/blog/top-20-cyberattacks-ics

[13] Caleb Henry; *Northrop Grumman's MEV-1 servicer docks with Intelsat satellite*, February 26, 2020, https://spacenews.com/northrop-grummans-mev-1-servicer-docks-with-intelsat-satellite/

[14] DHS CISA; *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organization,* December 2020,https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[15] NASA Office of the Chief Engineer; *Space System Protection Standard*, November 5, 2020 https://standards.nasa.gov/standard/nasa/nasa-std-1006-wchange-1

[16] OWASP; *C1: Define Security Requirements*, https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements

[17] Bailey, Brandon; *Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices*, October 2020.

[18] *RFC 4949 – Internet Security Glossary v2*, https://tools.ietf.org/html/rfc4949

[19] *Committee on National Security Systems (CNSS) Glossary*, https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[20] Dr. Tibor Schonfeld*, Adversary Threat Model for Requirements, Acquisition and Cybersecurity Engineering, June 2015*

[21] NIST *Guide for Conducting Risk Assessments rev 1,* September 2012 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[22] National Air and Space Intelligence Center; *Competing in Space,* January 2016, https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

Appendix C: Acronyms

Table 8: Acronyms

AC	Access Control
AD&C	Attitude Determination & Control
ASIC	Application Specific Integrated Circuit
ATO	Authorization to Operate
AU	Audit and Accountability
C&DH	Command and Data Handling
CARD	Cyber Assessment and Research Department
CM	Configuration Management
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial off-the-shelf
CPUs	Computer Processing Units
CSF	Cybersecurity Framework
CSS	Cybersecurity Subdivision
CUI	Controlled Unclassified Information
CVEs	Common Vulnerabilities and Exposure
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DAR	Data-at-Rest
DDOS	Distributed Denial-Of-Service
DIT	Data-in-Transit
DMZ	Demilitarized Zones
DOD	Department of Defense
EMSEC	Emissions Security
EPS	Electrical Power Subsystem
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOSS	Free and Open-Source Software
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GOTS	Government off-the-shelf
IA	Identification and Authentication
ICS	Industrial Control Systems
IDE	Integrated Development Environment
IDS	Intrusion Detection System

IR	Incident Response
I/O	Input/Output
IP	Internet Protocol
IPS	Intrusion Protection System
IT	Information Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security System
OPSEC	Operational Security
OS	Operating System
PPP	Program Protection Plan
RF	Radio Frequency
RMF	Risk Management Framework
RoT	Root of Trust
SBC	Single Board Computer
SBU	Sensitive but Unclassified
SC	System and Communications Protection Control
SDLS	Space Data Link Security
SDR	Software Defined Radio
SI	System and Information Integrity
SIEM	Security Information & Event Manager
S/C	Spacecraft
SP	Special Publication
SPD-5	Space Policy Directive – 5
STIG	Security Technical Implementation Guide
SV	Space Vehicle
TAPs	Test Access Points
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TRANSEC	Transmission Security
TT&C	Telemetry, Tracking, and Control
TTP	Tactics Techniques and Procedure

Cybersecurity Protections for Spacecraft: A Threat Based Approach

Cognizant Program Manager Approval:

Paul J. De naray, SYSTEMS
DIRECTOR NSS PROGRAMS
POLICY & OVERSIGHT
NATIONAL SPACE SYSTEMS
ENGINEERING DEFENSE SYSTEMS
GROUP

Aerospace Corporate Officer Approval:

Martin Whelan, SENIOR VP DEFENSE SYSTEMS GROUP
OFFICE OF EVP

Content Concurrence Provided Electronically by:

Brandon T. Bailey, SENIOR PROJECT
LEADER CYBER ASSESSMENTS &
RESEARCH DEPT CYBER SECURITY
SUBDIVISION ENGINEERING &
TECHNOLOGY GROUP

Technical Peer Review Performed by:

Benjamin Brostoff, SENIOR MEMBER OF TECHNICAL STAFF
SPACECRAFT SECURITY
CYBER DEFENSE SOLUTIONS
DEPARTMENT ENGINEERING &
TECHNOLOGY GROUP