Committee on National Security Systems

NATIONAL CYBERSECURITY INSTRUCTION FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

THIS DOCUMENT PROVIDES IMPLEMENTATION GUIDANCE. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION.

NATIONAL MANAGER

FOREWORD

1.   The Committee on National Security Systems (CNSS), pursuant to its authority under "National Security Directive 42" (Reference a), is issuing this instruction to provide guidance for implementing CNSS Policy (CNSSP) No. 12, *Cybersecurity Policy for Space Systems Used to Support National Security Missions* (Reference b).

2.   The primary objective of this instruction is to help ensure space system planners, developers, operators, Authorizing Officials (AO), Security Controls Assessors (SCA), program managers/information system owners, and cybersecurity practitioners both understand and ensure cybersecurity (cybersecurity) is adequately integrated into all components of space systems falling under the purview of Reference b.

3.   Additional copies of this instruction may be obtained from the CNSS Secretariat or the CNSS website: http://www.cnss.gov.

FOR THE NATIONAL MANAGER

/s/

MR. GREG L. SMITHBERGER

Acting, Deputy National Manager / NSA Director, Cybersecurity Directorate

TABLE OF CONTENTS

National Cybersecurity Instruction for Space Systems Used to Support National Security Missions

SECTION I – PURPOSE

1.   This instruction provides guidance to Reference b. In addition to this instruction, Reference b must be consulted when identifying applicable space system requirements.

2.   This instruction helps ensure the success of missions that rely on use of space-based National Security Systems (NSS). It elaborates on how to appropriately integrate cybersecurity 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. It also provides guidance to the AOs and SCAs for space systems with respect to their roles within the Risk Management Framework (RMF).

SECTION II – AUTHORITY

3.   The authority to issue this instruction derives from National Security Directive 42, which outlines the roles and responsibilities for securing National Security Systems, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives. Nothing in this Instruction shall alter or supersede the authorities of the Director of National Intelligence. This policy refers to NSA in the sense that the Director of the National Security Agency acts as the National Manager for NSS under NSD-42.

SECTION III – SCOPE

4.   This instruction applies to all entities within the scope of Reference b.

5.   CNSS has jurisdiction over NSS only; therefore, non-NSS components are not under the purview of Reference b or this instruction. Where NSS space systems form a part of a system- of-systems which includes non-NSS systems components, the mission owner and AO for such system-of-systems must consider the impact of non-NSS systems or components in their end-to- end analysis of risks. When practical and necessary, non-NSS systems or components should be selected that have security controls consistent with this instruction.

SECTION IV – REQUIREMENTS

6.   General.

  a. AO Reviews. The AO or the AO's designee must be afforded the opportunity to participate and make recommendations regarding the adequacy of cybersecurity measures at all major design reviews and major program decision points.

  b. Experiments, Tests, and Demonstrations. NSS space systems/components used for experiments, tests, or technology/capability demonstrations are required to implement security controls per this instruction. Consideration should be given to using experiments, tests, or demonstrations as a test bed to concurrently evaluate new security controls. The selection and implementation of security controls and the subsequent residual risk analysis should be based on an appropriate operational use case in order to facilitate rapid transition of subject space system/components to operational use. If an operational use case is not applicable or cannot be defined, security controls to protect the space system/components and the data collected from exploitation or attack must be implemented. The AO and mission owner for any experiment, test, demonstration, or follow-on operational use must explicitly accept any risks of not fully complying with this instruction.

  c. Security Controls Across the System Lifecycle. Special attention must be given to the fact that security requirements will vary for different components of a space system depending on when, where, and how those components are tested. Security controls needed for operations in flight may not be needed during system or component testing on the ground and vice versa. Data and physical connections not present or even possible while in flight will be established while the space system is on the ground. Security concerns with respect to physical access to the space system vary significantly depending on whether the system is in a pre- and post-launch environment. All the security implications of ground testing, storage, and transportation of space system components and of flight testing and operations must be addressed in the System Security Plan (SSP). The AO must approve the initial SSP and modifications to the SSP throughout the system's life cycle, ensuring the security control set is appropriate at each phase of the space system's life cycle and not solely for final operations in flight. The AO and program manager/information system owner must also ensure, through contracts, memoranda of agreement, service level agreements, etc., that appropriate security controls are applied to or by other systems and organizations when they logically or physically connect to or access the space system.

  d. Developmental Phase Security Concerns. The program manager/information system owner, in consultation with the information owner and mission owner, must develop a Program Protection Plan (PPP) describing how critical program information (CPI) and critical components (CC) will be protected in research, development, and acquisition of NSS space programs. The program manager/information system owner must present the PPP to the AO for review, who may forward the PPP to the acquisition milestone decision authority for approval. For any information system supporting research, development, and acquisition of NSS space systems, the PPP must be used to support the assigned information security policy, which determines information classification, information system categorization, and controls selection process or to support contract or service level agreement negotiations (e.g., cleared development contractor systems, commercial services,

etc.). Program managers/information system owners must request a Program Protection Implementation Plan from prime contractors to ensure protection requirements are passed to and implemented in all contractor locations. See Annex D for details on the PPP.

      e.   National Security Agency (NSA) Guidance and Assistance. Programs must engage NSA early in the acquisition lifecycle (i.e., during requirements development) in order to minimize the cost and schedule risks associated with identifying security requirements late in the program and having to repeat parts of the security evaluation processes. Early engagement ensures the planned security architecture is consistent with NSA cryptographic security and information systems security guidance and restrictions. Early engagement will minimize potential cost and schedule risks associated with security requirements, cryptographic algorithm selection, cryptographic device selection, and the associated cryptographic evaluation processes.[1]

      f.   Crypto Bypass.

      1)   Any capability designed into applicable space systems intended to bypass required cryptography (a.k.a. traffic crypto bypass) requires approval by NSA prior to Critical Design Review. Traffic crypto bypass must be designed in a manner to minimize the probability of inadvertent bypass activation due to malicious activity or failure of components. The program office must submit design information to the NSA early in the preliminary design phase and provide updates to the NSA as the design matures. Reference paragraph 14. b. of this document for additional design requirements.

      2)   The program office must include provisions for the NSA to review the implementation of operational systems such that NSA may assess implementation risks associated with the operational systems crypto bypass cybersecurity architecture. The program office must submit to the AO an artifact detailing any risks associated with using crypto bypass during system operations and test events. Risks associated with crypto bypass are subject to AO acceptance.

      g.   Body of Evidence (BOE).

      1)   The program office must provide, upon request of the AO, any BOE artifact for the purpose of making authorization decisions. Typically, in addition to the security authorization package (i.e., SSP, Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M)), the program office provides the following artifacts available to the AO:

      a)   System Concept of Operations or Operational Concepts Description

      b)   Authorization boundary diagram and description

      c)   Hardware, software, and firmware baseline inventory

---

[1] Vendors may engage NSA Cybersecurity Directorate through the Cybersecurity Business Affairs Office at: http://www.nsa.gov/ia/contacts/index.shtml#bao. Government organizations should contact their Department, Agency, or Service's Client Advocates at the NSA Cybersecurity Service Center. Further information can be found at: http://www.nsa.gov/ia/contacts/index.shtml#niasc.

        d)   Network diagram (showing all system components and internal/external connections)

        e)   Data flow diagram (aligned with network diagrams to show high-level data flows across major system components and the accreditation boundary)

        f)   Ports, protocols, and services (PPS) matrix (show all internal/external PPS; emphasize PPS crossing enclave boundaries)

        g)   Cross domain ticket number(s) for all cross domain solutions (CDS) (need connection approval)

        h)   Continuity of Operations Plan (or Business Continuity Plan, Disaster Recovery Plan, etc.)

        i)   Backup and Restoration Plan

        j)   Configuration Management Plan

        k)   Memoranda of Agreement/Understanding and Service Level Agreements

        l)   Risk Assessment Report

        m)   Security Controls compliance evidence

   2)   The BOE artifacts are contained or referenced in the SSP, SAR, and POA&M. The program office must ensure the SCA has access to all artifacts in the BOE. Annex E provides an exemplar list of BOE artifacts, with the types and specificity varying depending on the size, complexity, and maturity of the system.

   7. **Adequacy of Transmission Security (TRANSEC).** A System TRANSEC Plan (STP) must be developed, coordinated, and maintained in accordance with the instructions contained in CNSSP 31 and CNSSI 1031. The purpose of the STP is to ensure TRANSEC is appropriately addressed during space system developments and when space system services are leased or otherwise acquired. The STP provides the assigned AO concise documentation to support an adequacy review and adjudication of planned and/or implemented space system TRANSEC measures.

   8. **Supply Chain Risk Management (SCRM).** In accordance with CNSS Directive 505, *Supply Chain Risk Management* (Reference c), organizations must follow SCRM, systems security engineering, and risk management best practices and use SCRM tools and resources for all NSS space systems. Due to a space system's harsh operating environment, inaccessible platforms, and generally higher monetary value, traditional SCRM processes, tools, and techniques may not be practical in all situations (e.g. use of on-orbit security configuration management tools, etc.). To help minimize residual vulnerabilities and potential defects or deficiencies, organizations must pay particular attention to designing and building space platforms to higher standards and assurances and must implement the following SCRM requirements:

a.   Conduct an analysis of mission criticality for all NSS space system components and functions in accordance with United States (U.S.) Government, Department, or Agency directive and guidance documents.

b.   Apply supply chain protection measures to all NSS space systems in accordance with Reference c, CNSS Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems* (Reference d), and the Space Platform Overlay included in Reference d.

c.   Document all occurrences of suspect and confirmed counterfeit materiel in the appropriate reporting systems, to include the Government-Industry Data Exchange Program system.

d.   Identify potential incentives for commercial providers who voluntarily adopt NSS space system SCRM standards when commercially hosting NSS payloads and missions.

9.   **Commercial Space System Services.** Cybersecurity requirements must be included in commercial contract-related documentation. Department/Agency acquisition documentation must specify the following:

a.   What evidence the vendor must provide to give assurance they can comply with all cybersecurity requirements stipulated (e.g., at time of lease all security controls are implemented; system components are being maintained in the latest approved security configurations; FARS rules for cyber workforce requirements; cybersecurity-related plans, processes, and procedures are in place).

b.   Cybersecurity requirements (threshold and objective) requested and also the associated proposal evaluation criteria. (NOTE: See Annex G for additional details on security controls to include.)

c.   How the vendor will provide immediate notification if any proposed or contracted cybersecurity- related design, security controls, configuration, processes, or procedures change at any time during contract competition or after contract award, respectively.

d.   What cybersecurity-related artifacts are required and the degree of artifact detail the vendor must provide at the time of evaluation for source selection.

e.   The ways in which the vendor will be subject to government validation and inspection of the vendor's cybersecurity posture at any time during the lease for service.

f.   The contract proposal evaluation plan, which will define the cybersecurity evaluation criteria.

g.   Requirements for cybersecurity monitoring and reporting (reference paragraph 13).

h.   The ways in which the vendor will support government- and program-led

vulnerability and risk assessments, to include engagement with subject matter experts, access to documentation and proprietary information necessary to evaluate and mitigate residual risk.

10. Hosted Payloads.

a. Program managers/information system owners and AOs must identify and require implementation of additional security controls to mitigate the threats, vulnerabilities, and risks not readily identified during the hosting platform's requirements definition, design, and employment. If any security controls are not already implemented, they must be appropriately addressed by the respective program managers/information system owners to the satisfaction of their respective AOs.

b. When using hosting platforms, the government hosted payload organization must ensure cybersecurity strategies, SSPs, contracts, and memoranda of agreement address those requirements in Annex H.

11. Risk Assessment Model.

a. In accordance with CNSSP 22, Cybersecurity Risk Management Policy (Reference e), AOs must perform risk assessments for space NSS in accordance with the guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments* (Reference f).

b. AOs must perform and update risk assessments during each phase of a space system's life cycle. The life cycle of a space platform consists of the following phases: on-ground development, on-ground testing, pre-operational testing in space, operations in space, and decommissioning. As a minimum, risk assessments must:

1) Identify system vulnerabilities and the associated known and expected threats likely over the lifetime of the system that can exploit these vulnerabilities. This will help support accurate selection, tailoring, and implementation of baseline security controls in accordance with Reference d.

2) Identify and mitigate risks associated with the development phase of the lifecycle.

3) Determine the residual risk following security control assessments.

4) Determine, as part of continuous monitoring of authorized systems, the effect on risk due to changes to the system design or configuration, operational environment, operational concept or procedures, or threat sources' capability, intent, and targeting.

5) Determine risks resulting from space platform components disposal actions or surviving reentry.

c. The program/organization must identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations. For space platforms, the risk assessment must be performed as early as

possible to identify the anticipated space environment-unique threats/vulnerabilities (imposing risk) requiring mitigation during the space platform's pre-launch development. Programs should develop space system architectures, technologies, and procedures that can mitigate latent vulnerabilities and adapt to emerging threats.

    d.   The risk assessment must also consider that the information technology (IT) components control physical components of the space platform, and exploitation of any associated IT vulnerabilities can have immediate and catastrophic impacts to the space platform's functionality and supported mission. These unique risks must be identified in addition to all other types of risks. For examples of risks and lessons learned, consider similar non-space component control systems.

    e.   If risk assessments cannot be performed directly on the space platform, the developing organization must ensure that risk assessments are performed on a comparable article (e.g., flatsat, digital twin, cyber range.) that is operationally relevant, verified, and validated. The output of the test on the comparable article must be a verified and validated representation of cyber-compliance of the space platform's system security risk posture.

    f.   Appendices in CNSSI 1253, Security Categorization and Control Selection for National Security Systems (Reference d) provide exemplary tables, taxonomies, and inputs for risk factors applicable to typical IT systems. Some of that information does not apply to space systems, nor do the appendices consider the space-unique environment. Consequently, the AO (with the assistance of the ISSM) must ensure risk assessments for space systems modify and augment the tables and taxonomies information to account for the space-unique environment affecting the risk factors.

   12. Flight Termination System (FTS).

    a.   All links used for an FTS must implement mechanisms sufficient to ensure their availability, integrity, and confidentiality, as required by the mission. Remotely-controlled FTS must employ NSA-approved cryptography and cryptographic techniques to authenticate commands. Launch systems using remotely commanded FTS must implement NSA-approved cryptography for that application.

    b.   Autonomous FTS systems using Global Positioning System as an input must use Precise Positioning Service receivers with countermeasures against jamming and spoofing.

    c.   FTS hardware, software, and firmware must be developed, stored, and distributed in a manner that prevents inadvertent or intentional modification.

    d.   Autonomous flight termination systems (AFTS), also known as autonomous flight safety systems (AFSS), must use, at a minimum, the Global Positioning System (GPS) Precise Positioning Service (PPS), specifically Military Code (M-Code), in accordance with National Security Telecommunications and Information Systems Security Instruction 3006 (NSTISSI 3006), Operational Security Doctrine for the NAVSTAR Global Positioning System (GPS) Precise Positioning Service (PPS) User Segment Equipment (Reference g), and PL 111-383, Section 913, Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Reference h).

e.   See Annex I for additional guidance.

13. Cyberspace Defense

a.   Cyberspace Defense Services

1)   All NSS space systems and networks (to include the space, ground, launch, and user segments) and their associated critical support systems must be provided cyberspace defense services.

2)   Cyberspace defense services (whether government or commercial) must include: prepare, protect, detect, analyze, respond, and assess and adjust. Annex J provides descriptions of the services. For AO consideration and approval, responsible program managers/information system owners must provide in the system authorization package evidence of the service provider qualifications and ability to meet service execution and delivery.

3)   Cyberspace defense service activities must be coordinated as appropriate with network and space system operators, managers, owners, and users and with law enforcement, counterintelligence, and intelligence authorities.

b.   Information Security Continuous Monitoring (ISCM)

1)   NSS space organizations must implement a process to support ongoing monitoring of information security across the organization, consistent with NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Reference i).

2)   NSS space organizations must define a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people.

3)   Program offices must develop an ISCM strategy for each NSS space system consistent with the organizational ISCM strategy. The system ISCM strategy must demonstrate the ability to continuously monitor the security automation domains (and the related security controls) from Reference i.

4)   The system ISCM strategy must leverage information provided by Cyberspace Defense Service providers, as these providers are collecting, correlating, and analyzing security- related information from an enterprise-wide perspective, to include the sources and targets of attack/exploits, vulnerabilities across and specific to systems, and patches or upgrades necessary to thwart adversary efforts.

c.   Intrusion Detection and Prevention. Space NSS platforms must:

1)   Implement on-board intrusion detection systems (IDS) and intrusion prevention systems (IPS) capable of real-time monitoring, detecting anomalous activities, and responding to cyber threats.

2)   Implement IDS/IPS solutions out-of-band from the core space platform

operations to allow the ability to detect in the event of space platform compromise

       3) Implement continuous cybersecurity event logging, secure transmission of logged events to authorized ground stations, and automated alerting to appropriate response teams.

       4) Regularly update IDS/IPS threat signatures and anomaly detection algorithms based on threat intelligence and operational feedback.

    d. Commercial Space System Defense Services.

       1) If the Department/Agency requiring commercial services requires operations monitoring and control of those services, it must be identified in their contract language. Contract language must:

          a) Establish whether the vendor must provide a Network Operations Center (NOC) facility and an antenna in the space platform footprint to receive and monitor the signal.

          b) Establish whether the NOC must be staffed 24 hours per day, 7 days per week, and 365 days per year.

          c) Establish reporting procedures and parameters, to include:

             1.   Threshold for outages causing service interruption or degradation

             2.   Reportable events (e.g., outages escalating to an event)

             3.   Thresholds for when reporting must occur

             4.   Report formats

       2) Areas Departments/Agencies must consider for cybersecurity monitoring over the contract life include:

          a) Ensure cybersecurity compliance monitoring is outlined in initial acquisitions and leases.

          b) Establish in initial acquisitions that vendors must monitor and report changes of their cybersecurity posture in writing and provide details of how the changes affect the cybersecurity posture.

          c) The AO must initially establish the security controls for acquisition or lease, which of those security controls must be monitored, the frequency of monitoring, and by whom.

          d) Determine acceptable tools vendors may use to monitor for, manage, and report events and the format in which these tools must report events.

e. Space Platform Hardware Roots of Trust for Secure Boot. Space NSS platforms must:

1) Implement cryptographic trust for boot processes.

2) An operator must be able to restore or promote a space vehicle to a known trusted state of operation through a trusted boot process.

3) Ensure spacecraft hardware designs integrate hardware-based security components capable of cryptographically validating firmware and critical software during initial boot and runtime operations.

4) Verify system integrity at boot, during updates, and runtime operations.

5) Maintain chain-of-custody controls and trusted build pipelines during spacecraft hardware procurement, integration, and acceptance testing.

f. Secure Software Patch Development and Deployment. Space NSS platforms must:

1) Identify, prioritize, and remediate security vulnerabilities across the space system, including the space platform.

2) Ensure secure deployment and verification of software and firmware patches.

3) Verify the authenticity and integrity of all software and firmware patches, updates, and security configurations using cryptographic signatures sourced exclusively from trusted repositories and validated sources.

4) Configuration changes must also have strong security controls to protect against unauthorized changes and be completed in a secured and controlled manner.

g. Selection of Security Controls

1) Space platforms and payloads are comprised of information systems which, in the unique environment of space, require special consideration during security control selection. Security controls for applicable space platforms and payloads are selected and tailored in accordance with CNSSI 1253 Appendix-F Attachment-2 (CNSSI 1253F2), *Space Platform Overlay* (Reference j).

2) Information systems within the space, ground, and user segments of applicable space NSS may collect, generate, store, process, transmit, or receive classified information. Security controls for these information systems are selected and tailored in accordance with CNSSI 1253 Appendix-E Attachment-5 (CNSSI 1253E5), *Classified Information Overlay* (Reference k).

3) Information systems within the space, ground, and user segments of applicable space NSS may collect, generate, store, process, transmit or receive information

which must be protected within controlled access programs under the authority of the DNI. Security controls for these information systems are selected and tailored in accordance with CNSSI 1253 Appendix- F Attachment-4 (CNSSI 1253F4), *Intelligence Overlays* (Reference l).

        4)   The cognizant AO, in coordination with the System and Information Owner, and the National Cross Domain Services Management Office (NCDSMO) must validate requirements and proposed solutions for interconnecting security domains containing data of differing classification or releasability for applicable systems, in accordance with CNSSI 1253 Appendix-E Attachment-3 (CNSSI 1253E3), Cross Domain Solution Overlay (Reference m).

      h.   Cybersecurity Protections

        1)   Space systems and associated space vehicles supporting National Security Systems (NSS) functions must have strong cybersecurity measures to keep them safe and secure despite emerging cybersecurity threats. NSS must validate who can access or command them and use secured credentials to prevent impersonation or spoofing of authorized commanding entities, in accordance with EO 14144, Strengthening and Promoting Innovation in the Nation's Cybersecurity, January 16, 2025, and Space Policy Directive 5 (SPD-5), September 2020.

        2)   NSS space vehicles and equipment must implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all data, ensuring that data access is restricted to entities based on assigned roles and permissions and based on multi-factor authentication, with data only being accessible to assigned roles.

        3)   NSS space vehicles and equipment must ensure that entity entitlements are not misrepresented or spoofed to impersonate other entities and mislead authentication mechanisms.

        4)   Space systems must identify critical commands or critical command sequences that may be potentially harmful and use additional security mechanisms to protect these from inadvertent or unauthorized use.

        5)   The space platform must identify and authenticate all communications with external entities. All commands which have unrecoverable consequences must have stronger authentication, such as, two-person integrity or dual concurrence authentication, to confirm command execution. The space platform must verify command integrity and validate the command originated from an authorized entity.

        6)   The space system must maintain the confidentiality and integrity of information between the operator and the flight software module, from before transmission until after reception, in accordance with approved encryption methods.

        7)   Critical space vehicle functions should use enhanced security to maintain safety of operation and protect against malicious data corruptions, enforce access controls, verify software and command integrity, and verify only authorized entities can make changes.

8)   Authorized entities must be able to maintain control of a space vehicle either manually or automatically, regain control if lost, and take actions to prevent future loss of control or compromise.

9)   Maintaining cyber protections of space platforms and equipment is vital to preserving the integrity of NSS, space networks, and space environments. In the event of compromise, space systems must adapt to sustain mission capabilities and mitigate compromises from traversing to other elements within a system.

10) Space platforms and equipment must be able to distinguish between malicious use of a valid credential (including during autonomous operations) from actual authorized users (whether witting or unwitting).

11) Spacecraft launch operations must ensure that external ports are disabled prior to launch on the external bus.

14. **Cryptographic Requirements:** NSA-approved cryptography and cryptographic techniques, implementations, and associated security architectures, must be used wherever cryptography or cryptographic techniques are needed in applicable systems. At a minimum, they will be used to:

a.   Authenticate and encrypt all system commands and data from end to end (e.g., space platform bus and payload command echoes, telemetry, health and status, mission data, and communications relay) transmitted over any communications link that enters or leaves a space platform or that is accessible by unauthorized personnel or equipment in accordance with their classification or sensitivity unless otherwise indicated below. If the space platform uses more than one layer of encryption, then at least one layer of encryption must be from end to end, with possibly additional layers of encryption that might not be end-to-end (e.g., hop-to-hop). **Exception:** Data intended for immediate public release consistent with U.S. law or international agreements to which the U.S. is a party (e.g. World Meteorological Organization weather data agreements) do not require encryption. Methods to verify the integrity of the data generated, such as providing a hash value, should be considered.

b.   All space NSS communications that require cryptographic bypass types (i.e., Traffic, Metadata, Control & Status) must be coordinated with NSA. Command initiated or automatically invoked cryptographic traffic bypasses used to establish unencrypted communications with applicable space NSS must be approved by NSA. Metadata bypasses used to accommodate communication protocols and Control & Status bypasses used for data routing within the satellite must implement NSA recommended technical guidance and be approved by the cognizant system's AO.

1)   Traffic bypass is the capability to route data that would normally require encryption (e.g., commands, telemetry, mission data) around NSA-approved cryptography. Any capability designed into applicable space platforms to enable traffic bypass must:

a)   Reduce the likelihood of activation due to malicious acts and random

failures.

b)   Be submitted to NSA for review early in the preliminary design phase.

c)   Be approved by NSA prior to the system critical design review.

d)   Include provisions for NSA to review the implementation in the operational system to assess risks associated with the operational systems traffic bypass architecture. Risks identified by NSA must be corrected or accepted by the AO.

e)   Be made a matter or record, along with NSA's approval. This record will be provided to the cognizant AO to support their risk management decision.

2)   Metadata bypass is the capability to route portions of a communication protocol that do not require encryption (e.g., IP or CCSDS headers) around NSA-approved cryptography. Space platform architectures implementing metadata bypass must be approved by the cognizant system's AO, in coordination with NSA guidance.

3)   Control & Status bypass is the capability to adjust and monitor subsystem configurations (i.e., routing tables, modes of operation, etc.) by exchanging unclassified management data with payloads located outside of the Red/Black security boundary. The Control and Status bypass security architecture establishes dedicated internal space platform control plane communication paths to the subsystems that are on the black side of the NSA-approved cryptographic boundary. Space platform architectures implementing Control & Status bypass must be approved by the cognizant systems AO, in coordination with NSA guidance.

c.   Cryptographic keying material for systems employing classified or U.S. Controlled Cryptographic Item (CCI) equipment must be produced by NSA, or through an NSA approved process, and must, at a minimum, be protected and managed in accordance with CNSSI 4001, *Controlled Cryptographic Items* (Reference n), and CNSSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Materials* (Reference o). If deemed necessary, NSA will prescribe additional operational security doctrine to address handling instructions for specific cryptographic materials or products.

d.   Applicable systems employing other types of cryptographic equipment (i.e. those not produced or previously approved by NSA) must coordinate with NSA to obtain specific production, protection, and management instructions in order to receive NSA consideration for approval. NSA will perform or direct inspections of key distribution and storage facilities to verify adherence to applicable CNSS and/or NSA policy and instructions.

e.   Applicable systems employing NSA-approved cryptography or cryptographic techniques, must submit a system key management plan (SKMP) and relevant cryptographic security plans (CSP), written by the cognizant Department, Agency, commercial entity, or foreign government partner to NSA for approval.

1)   A SKMP describes the management of all keying material distributed through and employed by applicable systems, from the time it leaves the point of

generation until it is destroyed. At a minimum applicable systems must:

        a)   Coordinate with NSA prior to program initiation or development/acquisition contract award to ensure the key material requirements of the system can be satisfied.

        b)   Submit a SKMP for NSA review prior to the system preliminary design phase. If requesting keying material from NSA, SKMP approval must be received prior to placing the order.

        2)   A CSP describes the protection and recovery measures put in place for any cryptographic equipment, components, or keying material that may come into contact with or be operated in the presence of unauthorized personnel during the system's life cycle or due to a failed launch. At a minimum applicable systems must:

        a)   Submit a CSP for NSA review prior to the system critical design phase covering all phases of the system's life cycle where the potential for unauthorized personnel contact, or presence, with any cryptographic equipment, components, or keying material during operation is known. NSA approval must be received prior to the integration and test phase of development.

        b)   Submit a CSP for NSA review prior to the integration and test phase of development covering a failed launch or deorbited space platform. NSA approval must be received prior to shipment for launch.

        3)   Commercial partners ineligible to maintain a COMSEC Account for their use of classified or U.S. CCI cryptographic equipment, components, or keying material must contract for the services of an eligible third party COMSEC Custodian. The third party COMSEC Custodian will be responsible for developing and implementing the CSP to protect, manage, and control these commercial partners' cryptographic equipment, components, or keying material throughout their life cycle. See CNSSI 4005 (Reference q) for COMSEC Account eligibility and facility requirements.

    15. **Monitoring and Reporting.** NSS space systems must be monitored over time to manage risk and to maintain authorizations to operate, due to the dynamic nature of risk factors. Timely and accurate reporting of threats, vulnerabilities, and warnings must be disseminated within the government and with commercial partners as needed to ensure appropriate response and mitigations. Monitoring of NSS space systems is performed from operational, cybersecurity, system, and network perspectives. Reporting and monitoring from all of these perspectives are designed to accurately and completely determine the mission impact.

      a.   Unauthorized use of links: Unauthorized attempts to access space platform links (also known as bandwidth piracy) should be analyzed across all links. At the discretion of the AO, the space platform operator must implement security controls to prevent, monitor, attribute, and report unauthorized bandwidth usage to the mission owner.

      b.   Electro-magnetic interference (EMI): Departments/Agencies must establish capabilities and processes to support detecting, geolocating, reporting, and responding to

EMI that impacts the ability of NSS space systems to carry out their missions.

1) Technical controls to enable detection, geolocation, and response to EMI for new system developments must be considered during the system concept development phase. These high-level system requirements/capabilities must be developed by the cognizant requirements development entity during the system concept development phase.

2) In order to assure availability to authorized users, the AO, mission owners, and operations centers must pre-coordinate to:

a) Identify measures designed into the satellite system to detect, geo-locate, and resolve EMI events.

b) Identify operational controls to address any deficiencies in the detection, geolocation, and resolution of EMI.

c) Consider the use of capabilities external to the satellite system (such as terrestrial based Signals Intelligence (SIGINT) systems or overhead collection systems) to supplement the geolocation of EMI.

3) Develop and implement procedures to summarize and report EMI.

SECTION V - DEFINITIONS

Definitions are provided to clarify terms contained in this instruction, if they are not defined in Reference b or CNSSI 4009, *CNSS Glossary* (Reference p).

SECTION VI - REFERENCES

Future updates to referenced documents must be considered applicable to this implementation guidance.

Enclosures:
ANNEX A – DEFINITIONS
ANNEX B – ACRONYMS
ANNEX C – REFERENCES
ANNEX D – PROGRAM PROTECTION PLAN (PPP)
ANNEX E – BODY OF EVIDENCE (BOE) ARTIFACTS
ANNEX F – COMMERCIAL LEASE
ANNEX G – HOSTED PAYLOADS
ANNEX H – FLIGHT TERMINATION SYSTEM (FTS)
ANNEX I – CYBERSPACE DEFENSE SERVICES

ANNEX A

<u>DEFINITIONS</u>

1. <u>Anti-Jam</u>: The result of measures to resist attempts to interfere with communications reception.

2. <u>Anti-Signal Fingerprint</u>: Result of measures used to resist attempts to uniquely identify a particular transmitter based on its signal parameters.

3. <u>Anti-Signal Spoof</u>: Result of measures used to resist attempts to achieve imitative or manipulative communications deception based on signal parameters.

4. <u>Cover</u>: Result of measures used to obfuscate message externals to resist traffic analysis.

5. <u>Dual concurrence</u>: A form of authorization requiring two independent processes to authorize an action or event.

6. <u>Hosted Payload</u>: A payload carried and supported by a platform where acquisition and operation of the payload is under the authority of an organization different from the hosting platform.

7. <u>Host Platform</u>: A space platform that carries and supports a payload where acquisition and operation of the platform is under the authority of an organization different from the hosted payload.

8. <u>Low Probability of Detection</u>: Result of measures used to resist attempts by adversaries to recognize when a transmission is occurring.

9. <u>Low Probability of Intercept</u>: Result of measures used to resist attempts by adversaries to analyze the parameters of a transmission to determine if it is a signal of interest.

10. <u>Low Probability of Positioning</u>: Result of measures used to resist attempts by adversaries to determine the location of a particular transmitter.

11. <u>Program Protection Plan</u>: A risk-based, comprehensive plan to protect critical program information and critical components associated with a program throughout the research, development, and acquisition phase.

12. <u>Traffic Flow Security</u>: Result of measures used to conceal or obfuscate communication patterns.

ANNEX B

ACRONYMS

AO	Authorizing Official
BOE	Body of Evidence
CC	Critical Component
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COMSEC	Communications Security
CPI	Critical Program Information
EA	Electronic Attack
EMI	Electro-magnetic Interference
FTS	Flight Termination System
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
NSD	National Security Directive
NSS	National Security System
OPSEC	Operations Security

OSI	Open Systems Interconnection
POA&M	Plan of Action and Milestones
PPP	Program Protection Plan
PPS	Port, Protocol, and Service
RMF	Risk Management Framework
SAR	Security Assessment Report
SCA	Security Controls Assessor
SCRM	Supply Chain Risk Management
SIGINT	Signals Intelligence
SP	Special Publication
SSP	System Security Plan
STP	System TRANSEC Plan
TRANSEC	Transmission Security
U.S.	United States

ANNEX C

REFERENCES

a. National Security Directive 42 (NSD-42), *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

b. Committee on National Security Systems Policy 12 (CNSSP 12), *Cybersecurity Policy for Space Systems Used to Support National Security Missions*, August 2025.

c. Committee on National Security Systems Directive 505 (CNSSD 505), *Supply Chain Risk Management*, November 2021.

d. Committee on National Security Systems Instruction 1253 (CNSSI 1253) *Security Categorization and Control Selection for National Security Systems*, August 2022.

e. Committee on National Security Systems Policy 22 (CNSSP 22), *Cybersecurity Risk Management Policy*, September 2021.

f. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*, September 2012.

g. National Security Telecommunications and Information Systems Security Instruction 3006 (NSTISSI 3006), *Operational Security Doctrine for the NAVSTAR Global Positioning System (GPS) Precise Positioning Service (PPS) User Segment Equipment*, August 2001.

h. Public Law 111-383 (PL 111-383), *Ike Skelton National Defense Authorization Act for Fiscal Year 2011*, January 7, 2011.

i. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.

j. Committee on National Security Systems Instruction 1253 Appendix F Attachment 2 (CNSSI 1253F2), *Space Platform Overlay,* August 2025.

k. Committee on National Security Systems Instruction 1253 Appendix E Attachment 5 (CNSSI 1253E5), *Classified System Overlay,* September 2022.

l. Committee on National Security Systems Instruction 1253 Appendix F Attachment 4.2 (CNSSI 1253F4.2), *Intelligence Overlay,* November 2023.

m. Committee on National Security Systems Instruction 1253 Appendix E Attachment 3 (CNSSI 1253E3), *Cross Domain Solutions Overlay,* February 2023.

n. Committee on National Security Systems Instruction 4001 (CNSSI 4001), *Controlled Cryptographic Items,* August 2023.

o. Committee on National Security Systems Instruction 4005 (CNSSI 4005),

Safeguarding Communications Security (COMSEC) Facilities and Materials, August 22, 2011.

p. Committee on National Security Systems Instruction 4009 (CNSSI 4009), *CNSS Glossary*, updated March 2022.

ANNEX D

PROGRAM PROTECTION PLAN (PPP)

1.   Background: Many NSS space systems are developed in whole or in part on information systems maintained, controlled, and protected out of purview of the AO. Development often occurs in unclassified environments with little oversight or mandated protection. Subsequent classification of the information is difficult to assure, because it has been exposed to a high level of risk and potential for previous compromise. Even unclassified information must be protected due to sensitivity of aggregated information and because a compromise of the architecture, data flows, components, and configurations of NSS space systems may provide some advantage to the adversary.

2.   Critical components (CC) are or contain information and communications technology (including hardware, software, and firmware, whether custom, commercial, or otherwise developed) which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

3.   Critical program information (CPI) are elements or components of a program in the research, development, and acquisition phase that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. CPI includes information about applications, capabilities, processes, and end-items; elements or components critical to a system or network mission effectiveness; or technology that would reduce the U.S. technological advantage if it came under foreign control.

4.   To reduce the potential for information compromise, CPI and CC must be protected at equivalent levels during development and operations. Items to consider, on the information systems used to develop NSS space systems, may include defensive cyberspace service providers, monitoring and reporting of information compromises, processes for controlling information access, SCRM, Zero Trust principles, and residual risk posture.

5.   The PPP is used to develop tailored protection guidance for CPI and CC, and this guidance is disseminated and implemented throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI and CC protection activities throughout the Department/Agency. Following are key elements of a PPP, which are tailored to meet program requirements:

    a.   Technology and project description or system and program description with an emphasis on what is unique as the foundation for identifying CPI and CC.

      b. List of CPI and CC to be protected in the program. This generally describes classified CPI in an unclassified manner and is not suitable for horizontal protection analysis (i.e., across programs) or the preparation of a counterintelligence assessment.

      c. Threats to CPI and CC:
        1) Internal and external threats
        2) Summary of threat data from the intelligence community

      d. Vulnerabilities of CPI and CC to identified threats

      e. Countermeasures:
        1) Security countermeasures (all disciplines, as appropriate)
        2) Counterintelligence support plan
        3) Anti-tamper annex
        4) OPSEC plan
        5) System assurance
        6) Other countermeasures (unspecified)

      f. Technology assessment/control plan

      g. Classification guides

      h. Protection costs

      i. Follow-on support

ANNEX E

BODY OF EVIDENCE (BOE) ARTIFACTS

Below is a list of exemplar BOE artifacts, in addition to those identified in paragraph 6.g.1 of this instruction. The list below offers best practices and is neither mandatory nor all inclusive. It may be tailored early in system development to assist program managers/information system owners in identifying artifacts necessary to show compliance with assigned security controls. Some systems (e.g., systems in sustainment) may not have all the artifacts listed below. For RMF and connection decision purposes, the list of artifacts appropriate for a system at various points in its life cycle (to include upgrades and changes to fielded systems) should be coordinated with the AO and the SCA.

1. Data Requirements List

2. Clinger-Cohen Compliance Report

3. Communications Security (COMSEC) Material Control Guide

4. COMSEC Operational Security Doctrine

5. System TRANSEC Plan

6. System Key Management Plan (or Key Certificate Management Architecture)

7. Configuration Management Plan (developmental and operational)

8. Conformance Test Plan and Report

9. Program Protection Plan

    i. Incident Response Plan/Tactics, Technique and Procedures

    ii. Cybersecurity Strategy

    iii. Insider Threat Monitoring and Mitigation Strategy

    iv. Vulnerability Management Plan

    v. Patch Management Plan

10. Systems Engineering Documents:

    i. Interface Design Description

    ii. Cross Domain Appendix

    iii. Fail-Safe Design Analysis

    iv. System/Subsystem Detailed Design and Specification

11. System Documents:

   i.   Operating Procedures

   ii.   Operational Requirements Document

   iii.   Program and Budget Documentation

   iv.   Contracts and agreements with Developer/Contractor

12. System Test and Evaluation Documents:

   i.   Penetration Test Plan and Report

   ii.   Developer/Contractor plans, tests, and analysis

13. Security Assessment Report

14. Security Controls Compliance Evidence

   i.   Developer/Contractor test plans, analysis and reports

15. Software Documentation

   i.   Software Development and Installation Plan

   ii.   Software Test Plans/Procedures and Assurance Report

   iii.   Software User's Manual

   iv.   Version Description Document

16. TEMPEST Control, Test Plan and Report

17. Threat Studies and Analyses

ANNEX F

COMMERCIAL LEASE

1.   Departments/Agencies must determine the overall cybersecurity requirements and specific set of security controls most important to accomplishing their specific missions. Reference d and the Space Platform Overlay provide a starting point for identifying potential security controls for a commercial lease contract. Other security controls may be required beyond these. The controls will be applied and evaluated commensurate with the impact categorization identified in accordance with Reference d. Some areas to consider in selecting and tailoring the types of security controls for all components of a space system in the space, ground, user, or launch segments are any requirements in the lease associated with:

    a.   Physical and logical protection of fixed or mobile terrestrial-based facilities (e.g., satellite control facilities and ground stations such as NOCs, Teleports, etc.).

    b.   Continuity of operations for ground facilities.

    c.   Processing, storing, transmitting and/or receiving classified, proprietary, or other types of data not approved for public release.

    d.   Operations Security (OPSEC) measures to ensure anonymity of the Department/Agency from any of their third-party contractors.

    e.   Periodic third-party validation of vendor facilities and personnel, and of security processes, procedures, controls, and configurations.

    f.   If required by the mission owner, the Department/Agency must stipulate in the contract that "non-preemptible" service is required. This ensures the Department/Agency's service is contractually obligated to be provided for the entire duration of the lease and cannot be stopped and provided to some other customer or user, otherwise the vendor is in breach of the contract.

2.   The contract proposal evaluation plan may contain minimum threshold and any objective requirements as determined by the applicable AO and mission owner prior to releasing requests for proposal (or equivalent document). The evaluation plan may indicate preference is given to vendors who can meet threshold requirements and some established level of or all the objective cybersecurity requirements.

3.   The Federal Acquisition Regulations and the Defense Acquisition Regulations provide the requirements, processes, and sample documentation needed to process a commercial lease contract.

ANNEX G

<u>HOSTED PAYLOADS</u>

1.   Typically, hosted payloads and hosting platforms conduct acquisition, design, and development with differing levels of security requirements and controls. When non-NSS organizations (e.g. commercial, U.S. civil, or foreign) develop spacecraft and host an NSS payload, security risks to the NSS-payload are greater due to a lack of NSS organizational insight and control of the host platform's design, manufacture, and operation. Conversely, when organizations within the NSS community acquire and control both the payload and spacecraft, the requisite security controls are more likely to be already implemented.

2.   The following are requirements the government hosted payload organization addresses in cybersecurity strategies, SSPs, contracts, and memoranda of agreement, when using hosting platforms:

   a.   Process and procedures detailing how and when the hosting platform and hosted payload organizations share cybersecurity design/assurance information and determine how to share implemented cybersecurity capabilities.

   b.   Negotiated hosting platform security controls and related design changes necessary to mitigate serious risks to the hosted payload mission.

   c.   Security-related interface requirements.

   d.   Pre- and post-launch tests to verify cybersecurity functionality and status.

   e.   Cybersecurity requirements as an integral part of design reviews and decisions.

   f.   Identification and mitigation of significant cybersecurity risks associated with the payload's and hosting platform's external interfaces and communications links.

   g.   Development, review, and approval of a comprehensive cybersecurity architecture describing:

      1) Physical and/or logical separation of payload mission data from the host platform.

      2) Payload command and control data processing.

      3) Implementation of payload and platform COMSEC and TRANSEC.

      4) Data transmission to/from each communication link.

      5) Information flows between host platform and payload's space and ground segments.

      6) CDS requirements.

h.   Measures used to protect proprietary information (domestic or foreign), national security information, U.S. government information not approved for public release, and foreign government information.

i.   Procedures addressing foreign acquisition requirements as identified in applicable statutory and regulatory documents.

j.   Operational procedures for identifying, responding to, and recovering from attacks, anomalies, emergencies, and other security-impacting events.

k.   Potential incentives or preferences for commercial entities implementing host space platforms fully or partially compliant with CNSS cybersecurity requirements and meeting the hosted payload's protection requirements.

ANNEX H

FLIGHT TERMINATION SYSTEM (FTS)

1.   Flight termination includes actions to end the flight of an errant aerospace vehicle that either poses a threat to public safety or that must be prevented from leaving controlled areas to protect sensitive information or technology. FTS must be designed, built, and operated to reliably terminate errant aerospace vehicles and to prevent unwanted termination of aerospace vehicles.

2.   FTS fall into three categories: commanded, autonomous, and hybrid.

    a.   Commanded: In a commanded system, the decision to terminate a vehicle and the associated commands originate from a source outside the aerospace vehicle. Each system and link must be examined to determine the requirement for security controls. Reference b requires use of NSA-approved cryptography for launch vehicles using remotely-controlled FTS. FTS implementations lacking NSA-approved cryptography (e.g., Inter Range Instrumentation Group) are not authorized for the launch of spacecraft falling under the scope of Reference b.

    b.   Autonomous: Autonomous systems include many of the same components as commanded systems; however, the decision to terminate flight is made by the aerospace vehicle. Procedures must be in place to ensure the software and/or firmware remains unmodified from the reviewed and approved version. Confidentiality, integrity, and availability of links connecting these components must be examined to ensure adequate safety and mission assurance is provided. Use of Precise Positioning Service is required for all launch vehicles delivering NSS.

    c.   Hybrid: Hybrid FTS combine features of both commanded and autonomous systems. The security of hybrid FTS must meet the minimum requirements for both commanded and autonomous systems.

3.   Nearly every link requires integrity and availability controls, but careful consideration to system and link availability must be given to systems that allow the aerospace vehicle to continue or terminate based on a lack of inputs needed to make those decisions. Many FTS include safety mechanisms that block the execution of flight termination prior to leaving the launch complex or after the point where the vehicle can no longer pose a threat to safety or leave the controlled area. These features can be effective in reducing risks from adversary jamming and spoofing of data sources or command links early or late in the aerospace vehicles flight.

ANNEX I

CYBERSPACE DEFENSE SERVICES

Cyberspace defense services capabilities are described as follows:

1. Prepare: organize, develop processes and procedures, train, and equip (select and deploy)

2. Protect: maintain security posture, protect data, prevent malware, prevent unauthorized access, and contain or eradicate an attack

3. Detect: monitor and detect unauthorized or malicious activity

4. Analyze: determine if attacked (i.e., are network problems a result of malicious actions or benign actions/equipment failures), characterize attack (e.g., determine if a network outage is due to a computer attack and of what type or due to jamming of a communications link carrying the network), identify impacted systems and assets, perform damage assessments, and report incidents

5. Respond: develop course/s of action, implement changes to counter attack or mitigate, determine residual risk, and incident handling/collaboration

6. Assess and Adjust: assess services effectiveness and residual risk, implement changes, and conduct evaluations and assessments

Intrusion Detection and Prevention capabilities are described as follows:
1. Continuous Monitoring: Implement real-time observation and analysis of spacecraft telemetry and operational data to detect new cyber threats.
2. Vulnerability Assessment: Conduct regular scanning and thorough analysis of spacecraft systems, identifying security vulnerabilities and weaknesses to enable mitigation efforts.
3. Anomaly and Attack Detection: Employ mechanisms to identify unusual operational patterns and potential cyber-attacks through system behavior monitoring, telemetry analysis, and audit log evaluation.
4. Audit and Logging: Maintain logging capabilities to record, retain, analyze, and manage spacecraft system data. Logs shall support detection, incident analysis, and corrective actions.
5. Autonomous Recovery: Enable spacecraft systems to automatically transition into secure states upon detecting cyber threats, ensuring system safety and mission assurance.
6. Threat Mitigation: Establish measures and capabilities to mitigate or reduce impacts resulting from identified cyber incidents.
7. Forensic Logging: Ensure secure logging designed to facilitate forensic analysis and cyber incident attribution, enabling investigative and corrective capabilities.

Secure Boot capabilities are described as follows:
1. Cryptographic Root of Trust: Incorporate cryptographic hardware elements that provide a foundational trust anchor, ensuring software integrity and authenticity during spacecraft system boot processes.
2. Integrity Verification: Implement cryptographic mechanisms and verification processes to ensure software and firmware integrity at system boot, during operation, and throughout

updates.

Secure Software Patch Development and Deployment capabilities are described as follows:
1. Patch Deployment & Validation: Establish processes for securely deploying and cryptographically validating software and firmware patches before spacecraft system implementation.
2. Vulnerability Remediation: Develop processes for identifying, prioritizing, and remediating security vulnerabilities through validated and secure software updates.
3. Configuration Control: Maintain verified and secure configuration baselines to ensure spacecraft software and firmware remain protected against unauthorized modification.

Additional supporting capabilities include:

1. Secure Communication Management
   a. Communication Protection: Integrate protections against communication threats such as spoofing, jamming, and unauthorized access, and require encryption of all spacecraft communications to preserve confidentiality, integrity, and availability.
2. Authentication and Authorization
   a. Command Authentication: Implement cryptographic mechanisms to verify and authenticate all spacecraft commands and software/firmware updates, ensuring commands originate from authorized sources.
3. Secure Development & Supply Chain Assurance
   a. Supply Chain Security: Ensure secure sourcing, verification, and integration of spacecraft components and materials, protecting against supply chain compromises through appropriate controls, approved sourcing, and validation processes.