Committee on National Security Systems

CNSSP 12
August 2025

CYBERSECURITY POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

CHAIR

FOREWORD

1. The primary objective of this policy is to help ensure the success of national security missions that use space systems, by fully integrating cybersecurity into the planning, development, design, launch, sustained operation, and decommissioning of those space systems used to collect, generate, process, store, display, transmit, or receive National Security Information (NSI), as well as any supporting or related infrastructure.

2. Presidential Policy Directive 4 (PPD-4), *National Space Policy of the United States of America* (Reference a), states that the national security of the United States is critically dependent upon space capabilities and this dependence will grow. Space Policy Directive 5 (SPD-5), *Cybersecurity Principles for Space Systems* (Reference b), addresses the importance of space systems, stating "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." National Security Presidential Directive 40 (NSPD-40), *U.S. Space Transportation Policy* (Reference c), reiterates that space systems are critical to the defense of the Nation and access to space must be assured. Space activities are also closely linked to the operation of the United States Government's (USG) critical infrastructures and have increasingly been leveraged to satisfy national security requirements. As identified in Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization and Protection* (Reference d), and the Public Law 107-296 (PL 107-296), *Homeland Security Act of 2002* (Reference e), these critical infrastructures, include, but are not limited to, the information technology, telecommunications, power, and water distribution sectors. Executive Order 14028, *Improving Our Nation's Cybersecurity* (Reference f), and National Security Memorandum 8 (NSM-8) *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* (Reference g), further strengthen cybersecurity for the nation. Executive Order 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, (Reference h), calls for strengthening the cybersecurity of space National Security Systems (NSS) in specific ways.

3. With the continuing frequency, intensity, and adverse consequences of cyber intrusions, disruptions, and other threats to national security missions, the need for trustworthy NSS has never been more important to the long-term national security interests of the United States. Engineering-based solutions are essential to managing the growing complexity, dynamicity, and interconnectedness of today's systems, as exemplified by cyber-physical systems and systems- of-systems, including the space platform.

4. Knowing and understanding the current and projected full range of threats to these systems, and subsequent risk to national security, is of critical importance. Therefore, increased assurance and resilience are needed for the mission-essential functions of space systems supporting national security missions, including their supporting infrastructure, to help protect against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile means.

5. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: http://www.cnss.gov.

KATHERINE ARRINGTON

CNSS Chair

CNSS Secretariat, National Security Agency 9800 Savage Road, Ft Meade, MD 20755-6716, CNSS@nsa.gov

TABLE OF CONTENTS

CYBERSECURITY POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

SECTION I—PURPOSE

1. This document establishes national cybersecurity policy, provides minimum cybersecurity criteria, and assigns responsibilities for space NSS and services supporting space NSS as scoped below (hereinafter space NSS and services), that are used to support national security missions.

SECTION II—AUTHORITY

2. The authority to issue this policy derives from National Security Directive 42 (NSD-42), *National Policy for the Security of National Security Telecommunications and Information Systems* (Reference i), which outlines the roles and responsibilities for securing National Security Systems (NSS), consistent with applicable law, as amended, and other Presidential directives, executive orders, and memoranda.

3. Nothing in this policy alters or supersedes the authorities of the Director of National Intelligence (DNI).

SECTION III—SCOPE

4. This policy applies to space NSS and services, which includes:

a. All systems used by United States Government (USG) Departments and Agencies involved in the acquisition, development, lease, use, control, operation, or direct support of space systems and/or their components (e.g., launch systems, test ranges, space platforms, buses, payloads, operations centers, mission equipment, user modems/terminals/equipment, etc.) that, are or are intricately connected to, NSS (referred to collectively in this policy as "space NSS").

b. Services supporting space NSS that are developed, owned, operated, controlled, procured, or leased either by the USG or for the benefit of the USG by commercial entities (domestic and foreign) or foreign governments under bilateral or multilateral agreements or arrangements with the USG, which includes systems:

(1) Used to collect, generate, process, store, display, transmit, or receive National Security Information (NSI); and/or

(2) Used to collect, generate, process, store, display, transmit, or receive unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies; and/or

(3) Used to host or support applicable space platform payloads; and/or

(4) Used to experiment with, test, or demonstrate technology or capabilities for

current and future space NSS.

c. All information systems (whether USG, commercial, or foreign government) directly supporting or interfacing with space NSS and/or components thereof for development, integration, testing, launch, operations, maintenance, modification, control purposes, or decommissioning.

5. Where space NSS and services form a part of a system-of-systems which includes non-NSS or components, the mission owner and cognizant Authorizing Official (AO) for such system-of- systems, in coordination with the National Security Agency (NSA), must consider the impact of non-NSS components in their end-to-end analysis of risks. When practical and necessary, the AO may bring non-NSS or components under the scope of this policy.

6. Use of systems, or components, not originally planned, designed, or built to fully meet the requirements of this policy, and later designated or, by inter-governmental agreement or contractual action (e.g., lease), included within an NSS, will be contingent upon the cognizant AO's risk acceptance decision after performing a thorough review and comparison of alternatives, in coordination with NSA, to determine the solution that offers the best capability versus risk to meet mission needs.

7. This policy does not apply to operational ballistic missile weapons systems, munitions, and systems or platforms of any type not designed for space and usually operating at less than 100 kilometers (km) in altitude.

SECTION IV—POLICY

8. AOs, acquisition managers, program managers, architects, designers, system engineers, developers, integrators, planners, operators, maintainers, trainers, cybersecurity subject matter experts, and end users of applicable systems must ensure cybersecurity requirements are integrated and applied throughout the life cycle of space NSS and services as part of a holistic systems engineering approach. National Institute of Standards and Technology Special Publication 800-160 (NIST SP 800-160), *Systems Security Engineering* (Reference k), provides a guide for effectively integrating systems security engineering principles, concepts, and activities in to established systems engineering processes.

9. Space NSS and services must incorporate cybersecurity monitoring, auditing, and recovery measures to report related events to the cognizant AO and operations organizations.

10. Space NSS and services (singularly or as a system-of-systems) and their supporting infrastructure must be designed to adapt to evolving cybersecurity threats and operate through related attacks to the extent necessary to successfully execute national security missions. This capability must be periodically verified by initial/ongoing assessments, realistic tests, exercises, and/or modeling/simulation by the cognizant Departments and Agencies to ensure these systems have the requisite cybersecurity capabilities to successfully support operations as needed.

11. Foreign access to U.S. space capabilities and release of communications security (COMSEC) and other cybersecurity products to foreign governments must be controlled in accordance with PL 107-296 (Reference e) and Committee on National Security Systems

Policy 8 (CNSSP 8), *Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations* (Reference l).

12. All acquisitions, contracts, agreements, and leases; bilateral and multilateral foreign government agreements; and USG interagency agreements involving applicable systems must contain clauses that enforce the requirements contained in this policy.

13. The following cybersecurity requirements must be addressed and satisfied:

a. Space NSS and services, and their supporting infrastructure, contain information technology, information processing capabilities, and/or network technologies and must apply the Risk Management Framework (RMF) as part of an organization-wide Cybersecurity Risk Management Program (CRMP), established by a cognizant Department or Agency, in accordance with CNSSP 22, *Cybersecurity Risk Management* (Reference m).

b. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Reference n), provides a guide for the implementation of RMF and prescribes the roles and responsibilities of designated officials. There is no limitation to the designation of CRMP officials however, at a minimum, applicable systems must have a formally designated AO, Information System Security Officer (ISSO), and Security Control Assessor (SCA).

c. Commercial or foreign government systems not falling under existing USG authorities for authorization decisions must use a third party assessment organization acceptable to the cognizant AO and Department/Agency.

d. At a minimum, a cognizant AO's risk acceptance decision must be documented using the RMF core documents described in Committee on National Security Systems Instruction 1254 (CNSSI 1254), *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems* (Reference o).

e. Space NSS and services must identify and manage supply chain risk early and throughout the space NSS and services system life cycle through the use of acquisition and engineering mitigations informed by all-source supply chain threat information in accordance with Committee on National Security Systems Directive 505 (CNSSD 505), *Supply Chain Risk Management* (Reference p).

f. In accordance with CNSSI 1200, *National Information Assurance Instruction for Space Systems used to support National Security Missions* (Reference q), cybersecurity requirements and information systems security architectures for space NSS and services must be assessed by the cognizant AO, in coordination with NSA, prior to program initiation for new systems and prior to all major acquisition milestones.

g. Space NSS and services must meet the requirements of PL 113-283, *Federal Information Security Modernization Act of 2014* (Reference r), as a baseline, implement Executive Order direction, and be consistent with cybersecurity guidelines, standards, and

policies issued by the applicable Heads of USG Departments and Agencies having control, purview, or cognizance over the systems.

h. The security controls selected for space NSS and services must be derived from appropriate system security requirements, architectures, system designs, and risk assessments over the lifecycle of the system. Security controls are to be selected, tailored, implemented, assessed, and continuously monitored in accordance with CNSSP 22, *Cybersecurity Risk Management,* and CNSSI 1253, *Security Categorization and Control Selection for National Security Systems* (Reference s). Furthermore, the controls selected by the organization and the AO subsequently lead to both specification requirements and statement of work requirements in the systems engineering context. This leads to an iterative, cumulative, and recursive process of development. See CNSSI 1200 for additional guidance on selecting security controls using the CNSSI 1253 Appendices, as well as CNSSI 1253 Appendix-F Attachment-2 (CNSSI 1253F2), (Reference t) *Space Platform Overlay.*

(1) Continued advancement of adversarial threats may require revisiting risk tolerance thresholds and accordingly selecting and tailoring security controls over the lifecycle of a system. CNSSP 22 requires AOs to assess and continuously monitor security controls, based on risk assessments.

(2) Space NSS and services must implement cyber defense services, including on-board intrusion detection systems (IDS) and intrusion prevention systems (IPS), capable of real-time monitoring, detecting anomalous activities, and responding to cyber threats.

(3) Space NSS and services must implement a secure boot process using a hardware root of trust that enables an operator to restore or promote a space vehicle to a known trusted state of operation.

(4) Space NSS and services must implement a process to securely develop and deploy software and firmware patches and updates.

14. The following cryptographic requirements must be addressed and satisfied:

a. Authenticate and encrypt all system commands and data in Space NSS and services from end to end, in accordance with requirements and exceptions in CNSSI 1200. The system will use NSA-approved cryptography, in accordance with CNSSP 11 and CNSSP 15. The system must have a system key management plan (SKMP) and relevant cryptographic security plans (CSP) approved by NSA.

b. Any capability for unencrypted emergency backup links must be approved by NSA. Any other capability for cryptographic bypass must be coordinated with NSA and approved by the AO. See CNSSI 1200 for requirements.

c. Space NSS and services must implement TRANSEC measures in accordance with CNSSP 3 (Reference u) and a System TRANSEC Plan (STP) (Reference v) approved by the cognizant AO.

d. USG-owned and U.S. commercial-owned launch vehicles used to place in orbit space platforms falling within the scope of this policy must be equipped with a secure flight termination system (FTS). See CNSSI 1200 (Reference q) for more information on FTS.

SECTION V—RESPONSIBILITIES

15. The Director, NSA, as National Manager for NSS, shall, in accordance with CNSSD 502, *National Directive on Security of National Security Systems* (Reference w):

a. Review and approve all cryptographies, cryptographic techniques, commanded or automatically invoked cryptographic bypasses, as well as implementations of cryptographies, CSPs, and SKMPs intended to satisfy requirements associated with this policy.

b. Provide cybersecurity guidance and assistance to USG Departments and Agencies throughout their contracting processes for the design, development, manufacture, acquisition, launch, operation, and decommissioning of any applicable system requiring the use of NSA-approved cryptographies and cryptographic techniques.

c. Prescribe and issue additional security measures to protect classified and U.S. Controlled Cryptographic Items (CCI), cryptographic equipment, components, and keying material. These additional security measures must address, at a minimum, the recovery and/or destruction of any cryptographic- related material that is part of a failed launch or de-orbited space platform.

d. Issue, as requested, specific instructions and authorizations necessary for generating, protecting, and managing all cryptographic material for cryptographies that are neither classified nor U.S. CCI used in support of space NSS and services, and perform or direct random inspections of control facilities to verify the adherence to these instructions.

e. Establish and maintain a database of all applicable systems listing the NSA-approved cryptographies, their associated functions in each system's space platforms, and the compliancy status of each of these platforms to the requirements of this policy (based upon information provided to NSA by the cognizant USG Departments and Agencies).

f. In accordance with NSD-42 (Reference i), assist with the assessment of the overall security posture of applicable systems and identify cybersecurity related vulnerabilities.

g. Specify the format and information content of a CSP and SKMP to applicable Departments, Agencies, commercial entities, or foreign partners requesting employment of NSA-approved cryptography or cryptographic techniques.

16. Heads of USG Departments and Agencies must:

a. Ensure compliance with the requirements of this policy for the entire life cycle of all space NSS and services under their control, purview, or cognizance, as well as for any systems that directly support or interface with space NSS and services and/or components thereof. Compliance-related activities include:

(1) Ensuring applicable systems are integrated into the Department or Agency CRMP and are applying RMF in accordance with CNSSP 22 (Reference m). At a minimum ensure that:

(a) Cognizant system AOs, ISSOs, and SCAs are qualified, trained, and formally designated.

(b) The roles, responsibilities, and decision authority of designated officials are clearly defined.

(c) Risk acceptance decisions are documented in accordance with CNSSI 1254 (Reference o).

(2) Programming the funds required to acquire, implement, sustain, and decommission those products, services, measures, controls or techniques necessary to provide AO approved levels of cybersecurity.

(3) Ensuring cybersecurity products, services, measures, and controls are integrated, activated, and sustained.

(4) Coordinating system security architectures for applicable systems with the cognizant AO, and NSA, from program inception and periodically thereafter as the architectures evolve.

(5) Verifying with the cognizant AO, and NSA, that contracts to procure, lease, or develop applicable systems, components, or services comply with this policy.

(6) Verifying with the cognizant AO, and NSA, that any pre-existing system components or services comply with this policy before committing to their inclusion in the architecture.

(7) Ensuring applicable system SKMPs and CSPs are submitted to NSA for approval.

(8) Timely and accurate reporting to the cognizant AO, and NSA, concerning the compliancy status of applicable systems.

b. Through licensing, memoranda of agreement, or contracts, ensure the requirements of this policy are imposed on U.S.-, foreign government-, and commercially (domestic and foreign) owned systems involved in the launch, operation, maintenance, or decommissioning of applicable systems under their control, purview, or cognizance.

c. Ensure timely and accurate reporting of threats and vulnerabilities to the cognizant intelligence authority to support their dissemination of threat and vulnerability information.

d. Ensure applicable systems meet the requirements of PL 113-283 (Reference r).

e. Ensure compliance with the cyber incident detection, response, and reporting requirements of CNSSI 1010, *Cyber Incident Response* (Reference x).

f. Issue cybersecurity guidelines and standards, as appropriate, to include security assessment and authorization instructions for applicable systems under their control, purview, or cognizance.

g. Consult with NSA prior to initiating the development, acquisition, or purchase of cryptographies or cryptographic products for applicable space NSS to ensure they are suitable for the intended application and operational environment. See CNSSP 15, *Use of Public Standards for Secure Information Sharing* (Reference y) and CNSSP 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products* (Reference z), for more additional information.

SECTION VI—DEFINITIONS

17. Definitions of cybersecurity-related terms used in this policy are contained in CNSSI 4009, *Glossary* (Reference bb). All other definitions uniquely associated with this policy are defined in Annex A.

SECTION VII—REFERENCES

18. Referenced documents are listed in Annex B. Future updates to this policy precipitated by changes in the references must be promulgated as necessary.

Enclosures:
ANNEX A—Definitions
ANNEX B—References

ANNEX A

The terms in this policy are defined in CNSSI 4009 (Reference aa), except for those listed below.

DEFINITIONS

1. Bus: The infrastructure of a space platform typically consisting of the basic physical structures, mechanisms, and subsystems for propulsion, power, thermal control, attitude determination and control, and telemetry, tracking, and command (TT&C) communications and processing.

2. Flight Termination System: A capability designed and incorporated into launch vehicles providing for the deliberate termination of an anomalous launch process posing a threat to lives or property.

3. Launch Vehicle: The rocket or self-powered portion of the flight component of a space system used to propel itself and/or a space platform and its associated mission payload out othe earth's atmosphere.

4. Life Cycle: All phases of a system, to include research, planning, concept and architecture definition, design, development, demonstration, test and evaluation, deployment, operations, maintenance, product improvement, and system retirement.

5. NSA-approved Cryptography or Cryptographic techniques: Hardware, firmware, or software implementations of cryptographic protocols and algorithms reviewed and approved, certified and approved, or developed and approved by the NSA, the purposes of which are to protect national security information or systems in a specific application and intended operational environment.

6. National Security Mission: An activity that utilizes a national security system as defined in CNSS Instruction 4009, part (A)(i)(V).

7. Payload: A mission system/package providing specified products or services to users or customers that is carried and supported (e.g., power, TT&C interface) by a space platform. Multiple payloads may be integrated into a space platform.

8. Space: The region at least 100 km above the mean sea level of Earth.

9. Space Platform: A satellite, spacecraft, space vehicle, and relays, developed, launched, and operated for purposes of providing specified products or services to users or customers. A space platform operates at an altitude greater than 100 km and typically consists of a bus and one or more payloads.

10. Space System: A defined set of interrelated processes, communications links, and devices providing specified products or services to users or customers from a space platform(s), or directly necessary for the proper operation of the space platform(s). Examples of space system devices or components are space platforms; payloads; space bus/payload operations

centers; mission/user terminals for initial reception, processing, and/or exploitation; and launch systems.

11. Unauthorized Personnel: Personnel that have not met the standards for eligibility to access classified information in accordance with Executive Order 12968.

[1]See CNSSI 4009, *Glossary* (Reference bb).

ANNEX B

REFERENCES

a. Presidential Policy Directive 4 (PPD-4), *National Space Policy of the United States of America*, June 28, 2010.

b. Space Policy Directive 5 (SPD-5), *Cybersecurity Principles for Space Systems*, September 4, 2020.

c. National Security Presidential Directive 40 (NSPD-40), *U.S. Space Transportation Policy*, November 21, 2013.

d. Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization and Protection*, December 17, 2003.

e. Public Law 107-296 (PL 107-296), *Homeland Security Act of 2002*, November 25, 2002.

f. Executive Order 14028 (EO 14028), *Improving Our Nation's Cybersecurity*, May 12, 2021.

g. National Security Memorandum 8 (NSM-8), *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 19, 2022.

h. Executive Order 14144 (EO 14144), *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, January 16, 2025.

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

j. Executive Order 12333 (EO 12333), *United States Intelligence Activities*, July 30, 2008 (as amended).

k. National Institute of Standards and Technology Special Publication 800-160 (NIST 800-160), *Systems Security Engineering*, November 2016.

l. Committee on National Security Systems Policy 8 (CNSSP 8), *Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations*, September 2021.

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

n. National Institute of Standards and Technology Special Publication 800-37 (NIST SP 800-37 Rev. 2), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, December 2018.

o. Committee on National Security Systems Instruction 1254 (CNSSI 1254), *Risk Management Framework Documentation, Data Element Standards, and Reciprocity Process for National Security Systems*, August 2016.

p. Committee on National Security Systems Directive 505 (CNSSD 505), *Supply Chain Risk Management (SCRM)*, March 4, 2025.

q. Committee on National Security Systems Instruction 1200 (CNSSI 1200), *National Information Assurance Instruction for Space Systems used to Support National Security Missions*, August 2025.

r. Public Law 113-283 (PL 113-283), *Federal Information Security Modernization Act of 2014*, December 18, 2014.

s. Public Law 114-113 (PL 114-113), Section 303, *Federal Cybersecurity Workforce Assessment Act of 2015*, December 18, 2015.

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

u. Committee on National Security Systems Instruction 1253 Appendix F Attachment 2 (CNSSI No. 1253F2), *Space Platform Overlay*, August 2025.

v. Committee on National Security Systems Policy 31 (CNSSP 31), *Policy for a System Transmission Security (TRANSEC) Plan (STP) for National Security Systems*, April 2024

w. Committee on National Security Systems Instruction 1031 (CNSSI 1031), *Instruction for a System Transmission Security (TRANSEC) Plan (STP)*, June 2023.

x. Committee on National Security Systems Directive 502 (CNSSD 502), *National Directive on Security of National Security Systems*, December 16, 2004.

y. Committee on National Security Systems Instruction 1010 (CNSSI 1010), *Cyber Incident Response*, September 2021.

z. Committee on National Security Systems Policy 15 (CNSSP 15), *Use of Public Standards for Secure Information Sharing*, March 2025.

aa. Committee on National Security Systems Policy 11 (CNSSP 11), *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, March 2025.

bb. Committee on National Security Systems Instruction Number 4009 (CNSSI No. 4009), *CNSS Glossary*, March 2022.