Committee on National Security Systems

CNSSP No. 12
28 November 2012

NATIONAL INFORMATION ASSURANCE POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

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

CNSSP No. 12

CHAIR

FOREWORD

1. Presidential Policy Directive (PPD-4), *National Space Policy of the United States of America*, (Reference a) reiterates that United States national security is critically dependent upon space capabilities and this dependence will grow. 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. Therefore, increased assurance and resilience are needed for the mission-essential functions of national security space systems, including their supporting infrastructure, to help protect against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile means.

2. The primary objective of this policy is to help ensure the success of national security missions that use space systems, by fully integrating information assurance into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems. Fully addressing information assurance is especially important for the space platform portion of space systems, since any vulnerability in them normally cannot be eliminated once launched.

3. This policy supersedes Committee on National Security Systems (CNSS) Policy No. 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions*, dated 20 March 2007.

4. The CNSS Secretariat is tracking the status of the Member and Observer organizations' implementation of new and revised CNSS Issuances in order to create an Issuance Compliance Report. The Secretariat will oversee and administer this report process, which will be initiated 6 months following approval of this policy.

CNSS Secretariat (IE32). National Security Agency. 9800 Savage Road, STE 6716. Ft Meade, MD 20755-6716
Office: (410) 854-6805 Unclassified FAX: (410) 854-6814
CNSS@radium.ncsc.mil

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

/s/
TERESA M. TAKAI

CNSS Secretariat (IE32). National Security Agency. 9800 Savage Road, STE 6716. Ft Meade, MD 20755-6716
Office: (410) 854-6805 Unclassified FAX: (410) 854-6814
CNSS@radium.ncsc.mil

NATIONAL INFORMATION ASSURANCE POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS

SECTION I—PURPOSE

1. This document establishes national information assurance policy, provides minimum information assurance criteria, and assigns responsibilities for space systems used to support national security missions.

SECTION II—AUTHORITY

2. The authority to issue this policy derives from National Security Directive 42, which outlines the roles and responsibilities for securing National Security Systems (NSS), consistent with applicable law, Executive Order 12333, as amended, and other Presidential directives.

3. Nothing in this policy shall alter or supersede the authorities of the Director of National Intelligence.

SECTION III--SCOPE

4. This policy applies to all USG Departments and Agencies involved in the acquisition, lease, use, control, operation, or direct support of NSS space systems and/or their components (i.e., launch systems, test ranges, buses, payloads, operations centers, mission equipment, etc.).

5. This policy is applicable to all NSS space systems and/or their components that are owned, operated, controlled, or leased either by the USG or for the benefit of the USG by domestic commercial entities or foreign governments under bilateral or multilateral agreements which includes systems:

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

b. Used to collect, generate, process, store, display, transmit, or receive unclassified information that requires security controls to protect it from public release, in order to deny an information advantage to those who may use the information to impact national interests; and/or

c. Used to test or demonstrate technology or capabilities for applicable space systems; and/or

d. Used to host or support applicable space payloads.

6. This policy is also applicable to all NSS systems (whether USG, commercial, or foreign) directly supporting or interfacing with applicable space systems and/or components thereof for development, integration, testing, launch, operations, maintenance, modification, control purposes, or deactivation.

7. 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 are specifically excluded from the requirements of this policy.

8. Use of space systems not originally planned, designed, nor built to fully meet the requirements of this policy, and later designated an NSS, shall be contingent upon the cognizant Authorizing Official's (AO) (formerly Designated Approval Authority (DAA)) risk acceptance decision after performing a thorough review and comparison of alternatives to determine the solution that offers the best capability versus risk to meet mission needs.

SECTION IV—POLICY

9. Space systems are critical to the defense of the nation, as stated in Reference a. Access to space must be assured in accordance with National Security Presidential Directive 40, *U.S. Space Transportation Policy*, (NSPD-40) (Reference e). Knowing and understanding the current and projected full range of threats to these systems, and subsequent risk to national security, is also of critical importance. Space systems are vital components of the nation's critical infrastructures, including, but not limited to, the information technology and telecommunications sectors, as identified in Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization and Protection*, (Reference f), and *Homeland Security Act of 2002*, (Reference g). Applicable space systems (either singularly or in combination with other systems) and their supporting infrastructure shall be designed to operate through information assurance-related attacks on them to the extent necessary to successfully execute any critical national security missions assigned to them. This capability shall be periodically verified by initial/ongoing assessments and realistic tests, exercises, and/or modeling/simulation by the cognizant USG Departments and Agencies to ensure the applicable space systems and/or system-of-systems have the requisite information assurance to successfully support mission operations as needed.

10. The following requirements shall be addressed and satisfied:

a. Acquisition managers, program managers, architects, designers, system engineers, developers, planners, operators, maintainers, trainers, information assurance subject matter experts, and end users of applicable space systems shall ensure information assurance requirements are integrated and applied throughout the life cycle of those systems.

b. Applicable space systems shall meet the requirements of Reference c, as a baseline, and be consistent with information assurance guidelines, standards, and policies issued by the applicable Heads of USG Departments and Agencies having control, purview, or cognizance over the systems.

c. National Security Agency (NSA)-approved cryptographies and cryptographic techniques, implementations and associated security architectures shall be used wherever cryptography or cryptographic techniques are needed in applicable space systems. At a minimum, they will be used to:

(1) Encrypt all data transmitted over communications links accessible by unauthorized personnel. Data releasable to the public does not require encryption.

(2) Provide pseudorandom bit streams to ensure transmission security (TRANSEC) effects are not predictable by unauthorized personnel.

(3) Authenticate and encrypt all system commands transmitted over communications links accessible by unauthorized personnel.

d. The information security controls specified in Committee on National Security Systems Instruction 1253 (CNSSI No. 1253) *Security Categorization and Control Selection for National Security Systems*, (Reference h), for applicable space systems shall be included in system design from inception.

e. TRANSEC measures shall be incorporated into the design of all applicable space systems as required to meet mission needs and to reduce security risks to an acceptable level over the operational life of the system. The system's AO shall adjudicate the adequacy of the TRANSEC measures during the preliminary design phase and again prior to system operation.

f. Information assurance requirements and information systems security architectures for applicable space systems shall be assessed by the cognizant security authorities during the Pre-Systems Acquisition Phase for new systems and prior to major acquisition milestones.

g. Memorandums of Agreement (MOAs), contracts, or leases with civil or commercial entities or foreign governments involving applicable space systems shall contain clauses that enforce the requirements contained in this policy.

h. Cryptographic material for systems employing U.S. Classified or Controlled Cryptographic Item (CCI) cryptographies shall be produced by NSA, or through an NSA approved process, and shall be protected and managed in accordance with NSA policy and instructions. Space systems employing other types of NSA-approved cryptographies shall require consultation with NSA to obtain specific keying material production, protection, and

management instructions. NSA shall perform or direct inspections of key distribution and storage facilities to verify adherence to applicable NSA policy and instructions.

i. Foreign access to U.S. space capabilities and release of communications security (COMSEC) and other information assurance products to foreign governments shall be controlled in accordance with Reference g, and CNSSP No. 8, *National 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 i).

j. The cognizant cross domain authority shall validate requirements and proposed solutions for interconnecting security domains containing data of differing classification or releasability for applicable space systems.

k. Applicable space systems shall be designed, developed, built, operated, and maintained under processes and oversight that minimize risks to acceptable mission assurance in accordance with Committee on National Security Systems Directive 505 (CNSSD No. 505), *Supply Chain Risk Management* (Reference j).

11. Applicable civil, commercial and foreign space systems employing NSA-approved cryptography or cryptographic techniques, shall implement a cryptographic security plan (CSP), written by the cognizant Department or Agency.

12. Prior to the launch of an applicable space system the cognizant Department or Agency shall develop a plan for the recovery and protection of any classified or U.S. CCI cryptographic equipment, components, or keying material that are part of a failed launch or deorbited space platform. The cognizant Department or Agency shall provide the plan to NSA for review and obtain approval prior to launch.

13. Applicable space systems containing information technology (IT), information processing capabilities, or network technologies shall undergo security assessment and authorization in accordance with CNSSP No. 22, *National Information Assurance Risk Management Policy for National Security Systems*, (Reference k), and shall have an AO, Information System Security Officer (ISSO), and Security Control Assessor assigned. Commercial or foreign government space systems not falling under existing USG authorities for security assessment and authorization shall employ a third party assessment organization acceptable to the cognizant AO and Department or Agency.

14. USG-owned and U.S. commercial-owned launch vehicles used to place in orbit space platforms falling within the scope of this policy shall be equipped with a secure flight termination system. Remotely-controlled flight termination systems must employ NSA-approved cryptographies and cryptographic techniques to authenticate commands.

15. Applicable space systems shall incorporate information assurance-related monitoring, reporting, and recovery measures to report information assurance-related events to the cognizant security/operations organization.

SECTION V—RESPONSIBILITIES

16. The Director, National Security Agency (DIRNSA), as National Manager of NSS security in accordance with Committee on National Security Systems Directive 502 (CNSSD No. 502), *National Directive on Security of National Security Systems*, (Reference l) shall:

a. Review and approve all cryptographies, cryptographic techniques, as well as implementations of cryptographies and CSP implementations intended to satisfy requirements associated with this policy.

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

c. Prescribe and issue, as required, additional security measures to protect U.S. CCI cryptographic equipment or components and keying material. These additional security measures shall 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 U.S. Classified nor CCI used in support of applicable space systems, 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 space 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 the responsibility in Reference b, assist with the assessment of the overall security posture of applicable space systems and identify information assurance-related vulnerabilities upon the request of the appropriate cognizant authority.

g. Specify the format and information content of a CSP to applicable civil, commercial and foreign entities requesting employment of NSA-approved cryptography or cryptographic techniques at the time of request.

17. Heads of USG Departments and Agencies shall:

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

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

(2) Ensuring information assurance products, services, measures, and controls are integrated, activated, and sustained.

(3) Coordinating system security architectures for applicable space systems with cognizant security authorities during program inception and periodically thereafter as the architectures evolve.

(4) Verifying with the cognizant security authority that contracts to procure, lease, or develop applicable space system components or services comply with this policy.

(5) Verifying with the cognizant security authority that any pre-existing system components or services comply with this policy before committing to their inclusion in the architecture.

(6) Timely and accurate reporting to cognizant security authorities concerning the compliancy status of applicable space systems.

b. Through licensing, memorandum of agreement, or contracts, ensure the requirements of this policy are imposed on U.S.-, foreign government-, and commercially-owned systems involved in the launch, operation, maintenance, or decommissioning of applicable space 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 as appropriate.

d. Ensure applicable systems meet the requirements of Reference c.

e. Issue information assurance guidelines and standards, as appropriate, to include security assessment and authorization instructions for applicable space systems under their control, purview, or cognizance.

SECTION VI—DEFINITIONS

18. Definitions of information assurance-related terms used in this policy are contained in Committee on National Security Systems Instruction 4009 (CNSSI No. 4009), *National Information Assurance Glossary*, (Reference m). All other definitions uniquely associated with this policy are defined in Annex A.

SECTION VII—REFERENCES

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

Enclosures:
ANNEX A—Definitions
ANNEX B—References

ANNEX A

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 TT&C (telemetry, tracking, and command) 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 of the 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 Cryptographies: Hardware, firmware, or software implementations of cryptographic algorithms reviewed and approved, or certified 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. 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.

7. Space Platform: A satellite, spacecraft, or space station 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 100km and typically consists of a bus and one or more payloads.

8. 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.

ANNEX B

REFERENCES

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

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

c. Public Law 107-347 (PL 107-347), E-Government Act of 2002, including Section III, *Federal Information Security Management Act of 2002*, December 17, 2002.

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

e. National Security Presidential Directive 40 (NSPD-40), *U.S. Space Transportation Policy*, December 21, 2004.

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

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

h. Committee on National Security Systems Instruction 1253 (CNSSI No. 1253), *Security Categorization and Control Selection for National Security Systems*, March 2012.

i. Committee on National Security Systems Policy 8 (CNSSP No. 8), *National Policy Governing the Release and Transfer of U.S. Government (USG) Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations,* August 27, 2012.

j. Committee on National Security Systems Directive 505 (CNSSD No. 505), *Supply Chain Risk Management*, March 7, 2012.

k. Committee on National Security Systems Policy 22 (CNSSP No. 22), *National Information Assurance Risk Management Policy for National Security Systems*, January 2012.

l. Committee on National Security Systems Directive 502 (CNSSD No. 502), *National Directive on Security of National Security Systems*, December 16, 2004.

m. Committee on National Security Systems Instruction 4009 (CNSSI No. 4009), *National Information Assurance Glossary*, updated April 26, 2010.