Committee on National Security Systems

CNSS Policy No. 12
20 March 2007

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

CHAIR

FOREWORD

1. National Security Presidential Directive (NSPD) No. 49, Subject: National Space Policy, dated 31 August 2006, states 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 U.S. Government's critical infrastructures, and have increasingly been leveraged to satisfy national security requirements. Based on the importance of these activities and increasing threats to them, it is imperative that the national-level information assurance (IA) space policy be updated, promulgated, and adopted, further ensuring the availability, confidentiality, authenticity, integrity, and survivability of the national security information environment under a wide range of peace or war time threat scenarios.

2. The primary objective of this policy is to ensure the success of national security missions that use space systems by fully integrating IA 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. Effective with its date of signature, this policy supersedes National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 12, National Information Assurance (IA) Policy for U.S. Space Systems (U//FOUO), dated January 2001.

3. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the Committee on National Security Systems (CNSS) Secretariat has initiated an Issuance Compliance Process for reporting annual status of Department and Agency implementation of new/revised CNSS Issuances. The first report for the attached policy, which will be promulgated by CNSS action memorandum, is due six months following its issuance.

4. Additional copies of this policy may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

//s//
JOHN G. GRIMES

CNSS Secretariat (I922). National Security Agency. 9800 Savage Road STE 6716. Ft Meade MD 20755-6716
(410) 854-6805. UFAX: (410) 854-6814
cnss@radium.ncsc.mil

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

SECTION I – SCOPE

1. This policy is applicable to all space systems launched, owned, operated, controlled, and leased by the United States Government (USG), or for the benefit of the USG by commercial entities (either domestic or foreign/international) and foreign governments, which;

a. are National Security Systems (NSS), and/or

b. are used to collect, generate, process, store, display, transmit, or receive national security information (NSI), and/or

c. are 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 threaten national security.

2. This policy is also applicable to all supporting or related NSS necessary for the proper operation of applicable space systems, and to all USG Departments and Agencies involved in the acquisition, launch, operation, maintenance, or lease of these space systems.

SECTION II – REFERENCES

3. Referenced documents are listed in Annex A. Any future updates to referenced documents impacting this policy shall be promulgated as necessary.

SECTION III – DEFINITIONS

4. Definitions of information assurance (IA) related terms used in this policy are contained in reference a. All other definitions uniquely associated with this policy are contained in Annex B.

SECTION IV – POLICY

5. Space systems are critical to the defense of the nation, as stated in reference b. Assured access to space must be protected in accordance with reference c. Space systems are important components of the nation's critical infrastructures, including, but not limited to, the information technology and telecommunications sectors, as identified in references d and e. Knowing and understanding the current and projected full range of threats to these systems is also of critical importance.

6. The following IA requirements shall be addressed and satisfied for applicable space systems:

a. Acquisition managers, program managers, architects, designers, developers, planners, operators, maintainers, trainers, and end users of applicable

space systems shall ensure that IA requirements are considered, funded, and adequately addressed throughout the life-cycle of those space systems.

b. Applicable space systems shall meet the requirements of the Federal Information Security Management Act (FISMA), reference f, as a baseline and, where appropriate, be consistent with IA guidelines and standards issued by the applicable Heads of USG Departments and Agencies having control, purview, or cognizance over them.

c. National Security Agency (NSA) approved cryptographies and cryptographic techniques shall be used to protect all communications links in applicable USG-owned or controlled space systems from exploitation, corruption, or denial consistent with mission requirements and the projected threat over the life cycles of these space systems. Information system security architectures for applicable space systems shall be coordinated with NSA at their inception, and periodically during their evolution.

d. NSA-approved cryptographies shall be used to encrypt and authenticate command uplinks of applicable commercial (domestic or foreign/international) and foreign government-owned space systems, the loss of integrity or availability of which may include the immediate and sustained loss of mission effectiveness, or delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Applicable remote sensing satellites shall employ cryptographies to encrypt downlinks that are commensurate with the confidentiality level (i.e., classified, sensitive, or public) of the data, imagery, products, or services to be obtained; the encryption shall be turned on as requested by the U.S. national security authority served.

e. Cryptographic keying material for applicable space systems employing U.S. Classified and Controlled Cryptographic Item (CCI) cryptographies shall be produced by NSA, and shall be protected and managed in accordance with NSA policy and instructions. Space systems employing other types of cryptographies shall require consultation with NSA to obtain specific keying material production, protection, and management instructions. Periodic inspections of control facilities shall be performed to verify adherence to these instructions.

f. The encryption aspects of foreign access to U.S. remote sensing space capabilities and release of IA products to foreign governments shall be controlled in accordance with references g and h.

7. As required, additional security measures to protect U.S. CCI cryptographic equipment or components, and keying material used in applicable space systems, shall be prescribed. 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.

8. Applicable space systems that are integrated components of larger net-centric architectures and contain information technology (IT), processing or network technologies shall undergo IA Certification and Accreditation (C&A) in accordance with reference i, and shall have an IA Officer (IAO), Designated Accrediting Authority (DAA), Certification Authority (CA), Program Manager (PM), and User Representative assigned.

9. USG-owned and U.S. commercial-owned launch vehicles used to place in orbit space platforms that fall within the scope of this policy shall be equipped with a Flight Termination System (FTS) that uses a Secure Command Destruct System (SCDS) employing NSA-approved cryptographies.

10. Subject to policy and guidance for space systems outside the scope of this policy, USG Departments and Agencies may wish to consider the requirements of this

policy for those space systems which (a) collect, generate, process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, (b) may be associated with the operation and/or maintenance of critical infrastructures, or (c) would incur prohibitive replacement costs.

SECTION V – AUTHORITIES

11. Consistent with their authorities and responsibilities set forth in references b, j, and k . The Secretary of Defense (SECDEF) and the Director of National Intelligence (DNI), after consulting with, as appropriate, the Secretary of State and other heads of Departments and Agencies, shall oversee compliance with the national security space guidelines of the United States. This includes IA of applicable space systems.

12. Any issues requiring further resolution between the SECDEF and DNI regarding satisfaction of this policy's requirements shall be referred to the National Security Council (NSC) for resolution, consistent with the requirements of references b, k, and l.

SECTION VI – RESPONSIBILITIES

13. The Director, National Security Agency (DIRNSA), as National Manager of NSS and IA in accordance with reference m shall:

a. Review and approve all cryptographies and cryptographic techniques, and their implementations, intended to satisfy requirements associated with this policy. This includes supporting adjudication of all systems security architectures for applicable space systems.

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

c. Prescribe, as required, additional security measures to protect U.S. CCI cryptographic equipment or components, and keying material used in applicable space systems. 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 security keying material for cryptographies that are neither U.S. Classified nor CCI used in support of applicable space systems, and perform periodic inspections of control facilities to verify the adherence to these instructions.

e. Establish and maintain a database of all space systems which are compliant with, non-compliant with, or exempted via approved waivers or DAA approval decisions, in part or whole, from the requirements of this policy. This database shall also list the NSA-approved cryptographies each space system employs. Access to the database shall be controlled through appropriate access control applications.

f. In accordance with the responsibility in reference k, assess the overall security posture of, and disseminate information on, threats to and vulnerabilities of applicable space systems.

14. 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, as well as for any related national security systems, under their control, purview, or cognizance. Compliance-related activities include:

1) Programming the funds required to acquire those products, services, measures, or techniques necessary to provide acceptable or desired levels of IA.

2) Ensuring that IA products, services, and measures are integrated, activated, and sustained as critical security components of those space systems.

3) Coordinating with NSA to verify that applicable, deployed space systems comply with this policy before entering into contractual processes for the services of those space systems.

4) Coordinating system security architectures for applicable space systems with NSA during program inception and periodically thereafter as the architectures evolve.

5) Timely and accurate reporting to NSA concerning the compliancy status of applicable space systems, including cryptographies used, DAA decisions, and waiver approvals.

b. Ensure, through licensing, memorandum of agreement, or contractual relationships, that the requirements of this policy are imposed on U.S. and foreign owned systems involved in the launch, operation, or maintenance of applicable space systems under their control, purview, or cognizance.

c. Determine whether this policy should be applied to those space systems under their control, purview, or cognizance that are outside the scope of this policy.

d. Provide timely and accurate input to NSA to support their dissemination of information on threats to and vulnerabilities of applicable space systems. Assist in the coordination of this information.

e. Adhere to the guidance of the Chief Information Officers (CIO) Council, in accordance with reference f, applicable to this policy.

f. Issue IA guidelines and standards, as appropriate, to include C&A instructions for applicable space systems under their control, purvie, or cognizance, and ensure that IAOs, DAAs, CAs, and User Representatives are assigned for these systems.

SECTION VII – QUALIFICATIONS, EXCLUSIONS, AND EXCEPTIONS

15. This policy establishes minimum requirements for providing IA of space systems, or related systems that support U.S. national security missions. Depending on threats and risk management deliberations and decisions, heads of USG Departments and Agencies may impose more stringent requirements on the operation of their systems.

16. This policy does not apply to space systems that were past the initiation point of their preliminary design phase when this policy became effective, with the following exceptions:

a. This exemption does not automatically apply to any subsequent major redesigns of these space systems. The program managers responsible for the redesigns shall request that their Department/Agency review the proposed major redesigns, the results of which shall be submitted to the SECDEF and DNI, to determine if this policy should apply.

b. The SECDEF and DNI may revoke this exemption on a case-by-case basis for such space systems if the potential IA related risks to the space system clearly outweigh the cost and schedule impact of fully complying with this policy.

c. Space systems shall adhere to the requirements of reference f regardless of when their programs were initiated.

d. Any use of commercial (domestic or foreign international) or foreign government-owned space systems that were not originally planned, designed, nor built to fully meet the requirements of this policy shall be contingent upon the cognizant DAA's risk acceptance decision after performing a thorough review and comparison of alternatives to determine the solution that offers the best capability versus risk ratio to meet mission needs.

17. Any waiver processes incorporated into USG Departments' or Agencies' doctrine implementing this policy shall be applied on a case-by-case basis, and shall be applied in a manner ensuring that the national security posture of the U.S., its allies, and coalition partners, is not diminished. Granting authority is the CNSS Executive Agent.

18. Aircraft, operational ballistic missile weapons systems, munitions, and sub-orbital test vehicles are specifically excluded from the requirements of this policy.

19. Nothing in this policy should be interpreted as altering or superseding the existing authorities of the DNI.

Encls:

Annex A
Annex B

ANNEX A – REFERENCES

a. Committee on National Security Systems Instruction 4009 (CNSSI 4009), National Information Assurance Glossary, 2006 and future revisions.

b. National Security Presidential Directive 49 (NSPD-49), National Space Policy, August 31, 2006.

c. National Security Presidential Directive 40 (NSPD-40), U.S. Space Transportation Policy, January 6, 2005.

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, January 1, 2003.

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

g. National Security Presidential Directive 27 (NSPD-27), U.S. Commercial Remote Sensing Policy, April 25, 2003.

h. Committee on National Security Systems Policy (NSTISSP No. 8), National Policy Governing the Release of INFOSEC Products or Associated INFOSEC Information to Foreign Governments, February 13, 1997

i. Committee on National Security Systems Policy 6 (CNSSP 6), National Policy on Certification and Accreditation of National Security Systems, October 2005.

j. Executive Order 12333 (EO 12333), United States Intelligence Activities, December 4, 1981.

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

l. National Security Presidential Directive 1 (NSPD 1), Organization of the National Security Council System, February 13, 2001.

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

ANNEX B – DEFINITIONS

1. *Command Up-Link*: Data transmission path established for purposes of positioning or relocating space platforms (i.e., orbital insertions or adjustments), or for effecting tasking changes to the satellite, its subsystems, or mission payload(s).

2. *Critical Infrastructures*: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. These critical infrastructures include cyber, telecommunications, and physical infrastructures.

3. *Downlink*: Data link from a space platform to a ground or airborne platform.

4. *Flight Termination System (FTS)*: A capability designed and incorporated into launch vehicles which provides for the deliberate termination of the launch process that has been determined to be anomalous, and which might pose a threat to lives or property if the launch is not terminated.

5. *Information Assurance Officer (IAO)*: A government official assigned to the staff of system or enclave program managers, with the responsibility to ensure the proper development and integration of IA throughout the system or enclave life-cycle.

6. *Information Systems Security Architecture*: A strategic information asset base that defines the mission, the information necessary, the technologies necessary, and the transitional processes necessary for implementing the protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats.

7. *Launch Vehicle*: The rocket or self-powered portion of the flight component of a space system that is being tested (i.e., research, development, testing and engineering (RDT&E) activities) or otherwise used in an operational context to propel itself or a space platform and its associated mission payload out of the earth's atmosphere.

8. *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.

9. *NSA-Approved Cryptographies*: Hardware, firmware, or software implementations of cryptographic algorithms that have been 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.

10. *Personnel Security*: Special considerations regarding the management of people in an IT security environment. This includes topics such as background investigations, rules of behavior, controlling access to sensitive information, separation of duties, rotation of duties, and separation from service.

11. *Physical Security*: The safeguarding of a cryptographic module or of cryptographic keys or other critical security parameters using physical means.

12. *Preliminary Design Phase*: The acquisition phase of a space system that increases confidence in system alternative(s) by assessing risk levels and projected performance at a detailed engineering level. Activities include efforts to mature technology and baseline management and definitization, which culminate in a preliminary design review.

13. *Protection*: The application, integration, and certification of products or services in a communications system or network for purposes of providing a desired level of confidence that transmitted information and associated systems and networks will be available on demand and free from malicious disruption or exploitation. The objective of protection is to satisfactorily achieve some or all of the components of Information Assurance.

14. *Secure Command Destruct System (SCDS)*: The cryptographic component of the FTS. An approved U.S. cryptography incorporated into the launch operations center and launch vehicle that provides a capability for the secure or authenticated transmissions of a flight termination command or the activation of the FTS.

15. *Space Platform*: An orbiting satellite, spacecraft, or space station developed, launched, and operated for purposes of providing specified products or services to users or customers.

16. *Space System*: All of the devices and organizations forming the space network. These consist of: spacecraft; mission package(s); ground stations; data links among spacecraft, ground stations, and mission or user terminals, which may include initial reception, processing, and exploitation; launch systems; and directly related supporting infrastructure, including space surveillance and battle management and/or command, control, communications, and computers.