Department of Defense

# INSTRUCTION

**NUMBER** 8581.01
June 8, 2010

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA) Policy for Space Systems Used by the Department of Defense

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 8581.1 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the guidance in DoDI 5025.01 (Reference (b)) and the authority in DoDD 5144.1 (Reference (c)).

b. Implements requirements of National Security Directive 42 (Reference (d)) by establishing IA policy and assigning responsibilities for all space systems used by the Department of Defense in accordance with Committee on National Security Systems Policy No. 12 (Reference (e)).

c. Supplements IA policy and requirements contained in DoDD 8500.01E (Reference (f)) and DoDI 8500.2 (Reference (g)).

2. APPLICABILITY

a. This Instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

(2) All DoD use of space systems and the components thereof (e.g., launch vehicles, satellites, payloads, launch and test ranges, satellite and network operation centers, and user

equipment) to receive, process, store, display, or transmit classified or unclassified DoD information requiring controls as outlined in Appendix 3 of DoD 5200.1-R (Reference (h)) and in Attachment 2 of Directive-type Memorandum 04-010 (Reference (i)). This includes all DoD-owned or –controlled space systems, and all DoD use of commercial (domestic and foreign), other U.S. Government (USG), and, subject to the terms of international agreements, foreign government-owned space systems and the components thereof.

b. This Instruction does not apply to:

(1) Aircraft, operational ballistic missile weapons systems, anti-ballistic missile systems, munitions, and suborbital test vehicles that do not have subsystems that are part of a space system. When subsystems exist that are part of a space system, this Instruction shall specifically apply to those subsystems.

(2) DoD-owned or controlled space systems or segments thereof that were past the point of program initiation on June 21, 2005. However, this exemption does not extend to any subsequent major redesigns of these systems or segments.

c. The scope of this Instruction includes the entire life cycle, acquisition through decommission, of space systems used by the Department of Defense.

d. Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of sensitive compartmented information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (Reference (j)) and other laws and regulations.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. All DoD-owned or controlled space systems shall comply with References (d), (e), (f), and (g), and shall meet the IA requirements described in the procedures section of this Instruction regardless of mission assurance category (MAC) or confidentiality level (CL).

b. All DoD use of commercial, other USG, or foreign government-owned space systems (i.e., those not owned or controlled by the Department of Defense) shall be in compliance with the IA requirements described in the procedures section of this Instruction.

c. A cryptographic security plan (CSP) shall be required for all space systems covered by this Instruction that have National Security Agency (NSA)-approved cryptography. The CSP shall, at a minimum, address all applicable security requirements related to the system's cryptography and keying material, including plans for the recovery and/or destruction of any cryptographic related material that is part of a failed launch or deorbited space platform. NSA shall specify the format and information contents of the CSP.

d. All programs acquiring DoD-owned or controlled space systems shall comply with DoDI 8580.1 (Reference (k)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8 EFFECTIVE DATE. This Instruction is effective immediately.

Cheryl J. Roby
Acting Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES


(a) DoD Directive 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," June 21, 2005 (hereby cancelled)
(b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(c) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(d) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990[1]
(e) Committee on National Security Systems Policy No. 12, "National Information Assurance Policy for Space Systems Used to Support National Security Missions," March 20, 2007[2]
(f) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(h) DoD 5200.1-R, "Information Security Program," January 14, 1997
(i) Under Secretary of Defense for Intelligence Directive-Type Memorandum 04-010, "Interim Information Security Guidance," April 16, 2004
(j) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(k) DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004
(l) DoD Directive 5101.2, "DoD Executive Agent for Space," June 3, 2003
(m) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(n) Defense Federal Acquisition Regulation Supplement (DFARS), Section 239.7102-1
(o) DoD Directive O-8530.01, "Computer Network Defense (CND)," January 8, 2001
(p) Chairman of the Joint Chiefs of Staff Instruction 3170.01G, "Joint Capabilities Integration and Development System (JCIDS)," March 1, 2009
(q) DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
(r) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(s) Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008[3]
(t) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition
(u) DoD Directive 3600.01, "Information Operations (IO)," August 14, 2006
(v) Committee on National Security Systems Instruction No. 4009, "National Information Systems Security Glossary," revised June 2006[4]
(w) Chapter 82 of title 15, United States Code


[1] Available at http://www.iad.nsa.smil/
[2] Available at http://www.cnss.gov
[3] Available at http://www.dni.gov/electronic_reading_room/ICD_503.pdf
[4] Available at http://www.cnss.gov

(x) Defense Acquisition University Glossary of Defense Acquisition Acronyms & Terms, 12th Edition, July 2005[5]

[5] Available at http://www.dau.mil/pubs/glossary/12th_Glossary_2005.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall oversee implementation of this Instruction and monitor all IA activities related to space systems used by the Department of Defense.

2. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L), when serving as the milestone decision authority (MDA) of space systems or systems that interact with space systems, shall oversee and monitor IA in coordination with ASD(NII)/DoD CIO, including conducting independent evaluations of program performance and resource requirements.

3. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in coordination with ASD(NII)/DoD CIO, shall oversee and monitor implementation of this Instruction for space system components that collect and process intelligence information.

4. DIRECTOR, NSA. The Director, NSA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, shall:

a. Keep the ASD(NII)/DoD CIO and the Secretary of the Air Force, acting as DoD Executive Agent (EA) for Space as designated by DoDD 5101.2 (Reference (l), apprised of all IA initiatives and activities affecting DoD space programs.

b. Plan, budget for, and develop guidance for research, development and engineering programs needed to protect future space systems to be developed and/or used by the Department of Defense and coordinate those activities with the Director, Defense Research and Engineering.

c. Evaluate and certify cryptography used in DoD-owned or controlled space systems. Provide data on this cryptography-related evaluation and certification to the system certification authority to support certifying the overall security of the space system.

d. Oversee the planning, development, and production of space-specific cryptography for which NSA has certification responsibility.

e. Develop and produce cryptographic components for space when requested and funded per agreement between NSA and the DoD Components.

f. Review and approve, as appropriate, DoD Component proposals to initiate and manage the development of cryptographic products for space systems. Provide oversight and technical

guidance to approved Component cryptographic development efforts leading to NSA evaluation and certification.

g. Provide guidance to the ASD(NII)/DoD CIO, the USD(AT&L), the DoD EA for Space, and the Heads of the DoD Components on the acquisition, integration, and life-cycle support of IA products, services, measures, and techniques for space systems used by the Department of Defense.

h. Provide information system security engineering (ISSE) support and guidelines to DoD space system programs beginning with concept and technology development, and continuing throughout their life cycle, to assist and guide DoD space program efforts.

i. Perform end-to-end, system security evaluations on space systems used by the Department of Defense when requested by the ASD(NII)/DoD CIO, the DoD EA for Space, the USD(AT&L), or the Commander, United States Strategic Command (CDRUSSTRATCOM), to assist in identifying IA-related vulnerabilities, assurances, threats, and risks.

j. Assist the Director, Defense Intelligence Agency (DIA), in development and review of system threat assessment reports (STARs) and capstone threat assessments (CTA) by providing all-source, all-classification level information operations (IO) threat data collected by NSA related to space systems.

k. Ensure the full inclusion of space systems IA architectures within the IA component of the overall Global Information Grid (GIG) architecture.

l. Maintain reports and other pertinent information provided by commercial, other USG, or foreign government-owned (i.e., those not owned or controlled by the Department of Defense but used by the Department of Defense) space system owners or service providers describing the IA measures taken to protect their systems.

m. Specify the format and information content of the CSP dependent on the type of space system (e.g., DoD-owned and controlled, commercial, other USG, foreign government-owned); review, comment on, and adjudicate CSPs submitted for approval.

5. DIRECTOR, DIA. The Director, DIA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, shall:

a. Review STARs for individual DoD space systems during their development to ensure that the full-range of applicable current and projected IO threats has been included. These assessments shall be DIA validated and include threats based upon all-source, all-classification-level threat data collected by the Intelligence Community (IC). The threat assessment shall also include DoD enterprise-wide threat sources if applicable, such as in situations where interconnections or trust relationships with the GIG are required.

b. Maintain and validate a space CTA to assess the threats for generic mission and/or orbit-specific platforms that do not meet the threshold defined in DoDI 5000.02 (Reference (m)) to require the production of a system specific STAR. The space CTA shall be prepared under the auspices of a DIA/Defense Warning Office and National Air and Space Intelligence Center co-chaired Threat Steering Group. The space CTA represents the validated DoD IC position and constitutes the primary threat assessment for use in the defense system acquisition process. The space CTA shall be updated and validated every 2 years.

6. DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA). The Director, NGA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 7 of this enclosure, shall act as the DoD Lead for all acquisition or exchange of commercial and/or foreign government-owned imagery-related remote sensing data for the DoD Components.

7. HEADS OF THE DOD COMPONENTS. The Heads of the DoD Components shall:

a. Ensure space systems under their responsibility comply with this Instruction.

b. Ensure that solicitations, contracts, or formal agreements that are executed by DoD Components to acquire space systems covered by this Instruction from commercial, other USG, or foreign government-owned entities require compliance with this Instruction, pursuant to applicable acquisition or agreement regulations (e.g., References (k), (m), and DFARS 239.7102-1 (Reference (n)).

c. Coordinate with the Director, NSA, in developing appropriate IA-related language for such solicitations, contracts, or formal agreements

d. Ensure program managers for space systems under their responsibility include ISSE, crypto certification, and certification and accreditation (C&A) in their program plans, budgets, and contracts, as appropriate.

e. Ensure the validation of IA requirements for space systems that do not support joint and combined operations through appropriate requirement oversight authorities.

8. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Serve as the principal military advisor to the Secretary of Defense regarding IA for space systems.

b. Ensure, in coordination with the ASD(NII)/DoD CIO, the validation of IA requirements for space systems supporting joint and combined operations through the Joint Requirements Oversight Council.

c. Develop, coordinate, and issue IA policies, doctrine, and procedures for joint and combined space operations.

9. CDRUSSTRATCOM. The CDRUSSTRATCOM, in addition to the responsibilities in section 7 of this enclosure, shall:

a. Ensure development of defensive actions necessary to deter or defeat unauthorized activity (e.g., computer network attack and computer network exploitation) against DoD-owned or controlled space systems and their associated critical support systems, and minimize damage from such activities in accordance with DoDD O-8530.01 (Reference (o)).

b. Assign MAC, CL, and designated accrediting authorities (DAAs) for all DoD-owned or controlled space systems, and for the acquisition of services that involve the use of commercial, other USG, or foreign government-owned space systems, that support more than one DoD Component, including those that are at or beyond the point of program initiation. This shall be done in coordination with the Chairman of the Joint Chiefs of Staff, the program's MDA, and the Heads of the DoD Components that have an operational interest.

# ENCLOSURE 3

# PROCEDURES

This enclosure provides the basic procedures for implementing IA for all space systems used by the Department of Defense.

a. Procedures for DoD-owned or controlled space systems, regardless of MAC or CL:

(1) Requirements for IA capabilities for systems supporting joint and combined operations shall be validated through the Joint Requirements Oversight Council in accordance with Chairman of the Joint Chiefs Instruction 3170.01F (Reference (p)). IA requirements for all other systems shall be validated through the appropriate Military Department requirements oversight authority.

(2) IA requirements for all DoD-owned or controlled space systems shall be defined and updated throughout the system life cycle consistent with the IA Component of the GIG architecture and in coordination with the Director, NSA, space system program offices, and sustainment organizations. Space system IA requirements shall be sufficient to counter applicable IO threats that have been assessed and validated by DIA.

(3) DoD information shall be protected through the communications security measures and procedures set forth in DoDI 8523.01 (Reference (q)).

(4) Cryptographic considerations include:

(a) Both the selection and implementation of cryptography used to meet IA requirements shall be approved by the Director, NSA.

(b) Commands to DoD-owned or controlled space platforms shall be both encrypted and authenticated.

(c) Data generated onboard DoD-owned or controlled space platforms (e.g., telemetry, tracking, and commanding and payload-sourced data) shall be encrypted in accordance with its CL. All information within a communications stream transiting a space system is encrypted at its originating node as required in accordance with References (f) and (g).

(d) Booster telemetry links shall not be encrypted. Emergency backup links that are automatically invoked to rectify lost communications with malfunctioning satellites need not be encrypted.

(e) A flight termination system that uses a secure command destruct system employing NSA-approved cryptography shall be required for all launch vehicles used to deploy DoD-owned or controlled space platforms.

(f) Any capability designed into DoD-owned or controlled space systems to bypass, for any reason, cryptography required by this policy during system operation shall:

1. Minimize the probability of bypass activation due to either malicious acts or random failures.

2. Be submitted to the Director, NSA, for review and comments early in the preliminary design phase.

3. Be submitted to the Director, NSA, for final approval well in advance of the system critical design review to allow the Director, NSA, to respond with comments or approval prior to the system critical design review date.

4. Include provisions for the Director, NSA, to review how the bypass was actually implemented in the operational system to ensure that no flaws were introduced. Flaws identified by the Director, NSA review shall be corrected.

(5) All links (e.g., command uplinks, downlinks, and crosslinks) on DoD-owned or controlled space systems, regardless of transmission media (radio frequency, optical, etc.), shall have transmission security (TRANSEC) protection (e.g., anti-jam and traffic flow security) appropriate for the mission and the projected threat environment over the life of the system. TRANSEC protection measures used shall be reviewed both early in the space system development process and just prior to accreditation by the Director, NSA, who will advise the DAA and the system program manager as to their adequacy for the intended application.

(6) C&A considerations include:

(a) All components of DoD-owned or controlled space systems that are DoD information systems as defined in Reference (f) shall undergo IA C&A in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP) specified in DoDI 8510.01 (Reference (r)).

(b) Interconnections of IC systems with DoD space systems shall be certified and accredited in accordance with a process jointly developed by the ASD(NII)/DoD CIO and the DNI CIO. For those space system components that process unencrypted SCI or other intelligence information under the purview of the DNI, the C&A requirements of Intelligence Community Directive Number 503 (Reference (s)) shall apply.

(c) The interconnection of DoD space systems with systems of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and DoD IA policies. Variations shall be approved by the responsible Combatant Commander with advice from the DAA, and incorporated in the DIACAP package. Prior to agreeing to such interconnections, the responsible Combatant Commander or DAA shall contact the Director, NSA, regarding the releasability of any cryptographic equipment, key material, or technology that may be involved.

b. Procedures for Department of Defense use of commercial, other USG, or foreign government-owned space systems (i.e., those not owned or controlled by the Department of Defense):

(1) Cryptography

(a) Space systems implementing NSA-approved cryptography to encrypt and authenticate system commands shall be used when supporting MAC I or II DoD systems. While NSA approved cryptography is preferred for commercial, U.S. civil, or foreign government-owned space systems supporting MAC III DoD systems, cryptography generally commensurate with commercial best practices is acceptable for encrypting and authenticating commands.

(b) The use of space systems that implement NSA-approved cryptographies that are not U.S. classified or controlled cryptographic item cryptographies in space systems used by the Department of Defense shall require consultation with NSA to obtain specific keying material production, protection, and management requirements. Periodic inspections of control facilities may be performed to verify adherence to these requirements.

(c) The use, design, or modification of any capability that allows the bypass of any NSA-approved cryptography shall:

1. Minimize the probability of bypass activation due to malicious or unintentional acts or random failures.

2. Be submitted to the Director, NSA, for review and comments early in the preliminary design phase.

3. Be submitted to the Director, NSA, for final approval in advance of the system critical design review to allow the Director, NSA, to respond with comments or approval prior to the system critical design review date.

4. If approved by the Director, NSA, be made a matter of record, along with the approval. The record of this approval will be available to the responsible DAA in support of the DAA's risk management decision regarding whether to lease or negotiate use of a commercial, other USG, or foreign government-owned space system to support national security missions.

5. If encryption bypasses are not specifically under the control of the satellite owner and operator (e.g., teleports and communications earth stations not operated by the satellite operator), evaluation and approval shall be performed separately from this evaluation.

(d) DoD data that transits commercial, other USG, or foreign government-owned space systems shall be end-to-end encrypted in accordance with its CL.

(2) Data and Imagery Protection

(a) Director, NGA shall acquire commercial remote sensing data, imagery, products, or services that use commercial remote sensing systems with IA equipment, policies, and procedures that are commensurate with the CL (i.e., classified, sensitive, or public) of the information to be obtained. This shall include protecting both upper-tier data and imagery, and also exclusive USG use of and access to data and imagery. NSA-approved cryptography commensurate with the CL shall be used for the protection of data and imagery, and it shall be enabled or bypassed as requested by the Department of Defense.

(b) DoD organizations planning development of a remote sensing system jointly with a commercial remote sensing operator shall consult with the Director, NSA, for guidance on appropriate IA protection measures given the sensitivity of the data, imagery, products, or services to be provided by the new system.

(3) Risk Acceptance. DoD use of commercial, other USG, or foreign government-owned space systems that are not fully compliant with the requirements of this Instruction shall be contingent upon the cognizant DAA accepting the risk. The DAA shall first consider the assigned MAC and CL associated with the mission to support the risk management decision. The DAA shall then perform a review of the proposed space system's ability to meet IA requirements and select the system that offers the best capability versus risk ratio to meet mission needs, and that has an acceptable level of residual risk in accordance with Reference (e).

# GLOSSARY

## PART I. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| ASD(NII)/DoD CIO | Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer |
| C&A | certification and accreditation |
| CDRUSSTRATCOM | Commander, United States Strategic Command |
| CIO | Chief Information Officer |
| CL | confidentiality level |
| CSP | cryptographic security plan |
| DAA | designated accrediting authority |
| DIACAP | DoD IA Certification and Accreditation Process |
| DNI | Director of National Intelligence |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| GIG | Global Information Grid |
| IA | information assurance |
| IC | intelligence community |
| IO | information operations |
| ISSE | information system security engineering |
| MAC | mission assurance category |
| MDA | milestone decision authority |
| NSA | National Security Agency |
| SCI | sensitive compartmented information |
| STAR | system threat assessment report |
| TRANSEC | transmission security |

| | |
|---|---|
| USD(AT&L) | Under Secretary of Defense for Acquisition, Technology, and Logistics |
| USD(I) | Under Secretary of Defense for Intelligence |

## PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Instruction.

C&A. Defined in Reference (r).

certification authority. Defined in Reference (r).

command uplink. 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).

CL. Defined in Reference (g).

crosslink. A data link between space platforms.

crypto certification. Verification and validation that a crypto device, crypto module, or crypto software was designed, developed, documented, and tested in accordance with prescribed security requirements that are tied to specific use(s) and intended operational environment(s).

defense-in-depth. Defined in Reference (f).

DAA. Defined in Reference (r).

DIACAP package. Defined in Reference (r).

DoD-owned or controlled space system. Any space system where development or operation is funded or controlled (e.g., via outsourcing contract) primarily by the Department of Defense to support the DoD mission.

downlink. Data link from a space platform to a ground or airborne platform.

end-to-end IA system security evaluation. A comprehensive system analysis via system design and process reviews along with system and component level testing to uncover, identify, and document all IA-related vulnerabilities, weaknesses, and assurances.

external system. A system that is outside the intrinsic and commonly recognized boundaries of the system of interest (e.g., DoD space system). An example of an external system is a widely shared communications backbone or data network that a space system might interface with for communications or data services.

flight termination system. A capability designed and incorporated into launch vehicles (and unmanned airborne vehicles) which, in the event of anomalies that might pose a threat to lives, property, or the compromise of national security-related technology, provides for the termination of the launch process or flights.

GIG. Defined in Joint Publication 1-02 (Reference (t)).

IA. Defined in Reference (f).

IO. Defined in DoDD 3600.01 ((Reference (u)).

information system. Defined in Reference (f).

ISSE. Defined in Committee on National Security Systems Instruction No. 4009 (Reference (v)). Also, for the purposes of this Instruction, ISSE (also known as IA Engineering) is a sub-discipline under system engineering that considers the value of the information and information assets, threats to and vulnerabilities of those assets, and the affordability of IA solutions. ISSE considers all aspects of IA products, services, measures, and techniques needed to protect information systems and networks using a comprehensive, defense-in-depth approach that integrates the capabilities of personnel, operations, and technology to achieve an appropriate level of protection.

launch vehicle. The rocket or self-powered portion of the flight component of a space system that is being tested 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.

land remote sensing satellite. Defined in chapter 82 of title 15, United States Code (Reference (w)).

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.

MAC. Defined in Reference (f).

national security information. Defined in Reference (v).

national security system. Defined in Reference (v).

NSA-approved cryptography. Hardware, firmware, or software implementations of cryptographic algorithms which have been reviewed and approved, or certified and approved by the Director, NSA, the purposes of which are to protect national security or DoD sensitive information or systems in a specific application and intended operational environment.

program initiation. Defined in Defense Acquisition University Glossary of Defense Acquisition Acronyms & Terms (Reference (x)). For non-MDAP space programs, an equivalent program initiation event shall be used.

secure command destruct system. Defined in Reference (e).

SCI. Defined in Reference (v).

space platform. A satellite, spacecraft or space station developed, launched, and operated for purposes of providing specified services to users or customers.

space system. Defined in Reference (t).

TRANSEC. Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

uplink. A data link from a ground or airborne platform to a space platform.

user representative. Defined in Reference (r).