Committee on National Security Systems

CNSS Policy No. 14
November 2002

National Policy Governing the Release of Information Assurance (IA) Products and Services to Authorized U.S. Persons or Activities that are Not a Part of the Federal Government

This document contains information exempt from mandatory disclosure under the FOIA. Exemption 3 applies.

The information contained herein that is marked U//FOUO is for the exclusive use of the DoD, other U.S. government, and U.S. contractor personnel with a need-to-know. Such information is specifically prohibited from posting on unrestricted bulletin boards or other unlimited access applications, and to an e-mail alias.

This document prescribes minimum standards. Your department or agency may require further implementation.

Committee on National Security Systems

CNSS Policy No. 14

CHAIR

1. Information Assurance (IA) is the protection of information in information systems by ensuring its availability, integrity, authentication, confidentiality, and non-repudiation. Often, it is necessary to communicate securely with U.S. persons or activities that are not part of the U.S. Government. In such instances, it is the responsibility of both parties to ensure the confidentiality of the information being exchanged.

2. This policy assigns responsibilities and establishes the criteria to be applied when U.S. Government activities provide IA products and services, to other U.S. persons or activities that are not a part of the federal government. This policy supersedes NCSC 2, National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources, dated 7 July 1983.

3. Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this policy from the Secretariat.

4. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

John P. Stenbit

CNSS Secretariat (I42) . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

NATIONAL POLICY GOVERNING THE RELEASE OF INFORMATION ASSURANCE (IA) PRODUCTS AND SERVICES TO AUTHORIZED UNITED STATES PERSONS OR ACTIVITIES THAT ARE NOT A PART OF THE FEDERAL GOVERNMENT

SECTION I – APPLICABILITY AND SCOPE

1. This policy governs the release of Information Assurance [1] (IA) products and services to *U.S. persons or activities that are not part of the federal government* (hereinafter referred to collectively as *U.S. entities*). These U.S. entities include, but are not limited to, U.S. Government contractors and vendors; governments of states, cities, and other local jurisdictions; law enforcement activities of states, cities, and other local jurisdictions; and institutions of higher learning.

2. IA products that may be approved for release in accordance with the provisions of this policy include, but are not limited to:

a. Information systems security devices that have been evaluated and endorsed by the National Security Agency to secure national security systems;

b. Information Assurance (IA) and IA-enabled information technology products that have been evaluated and validated in accordance with the provisions of NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, dated January 2000;

c. Any keying material and software associated with the products referred to in paragraphs 2.a and 2.b, above;

d. Maintenance and technical manuals applicable to the hardware components of the products referred to in paragraphs 2.a and 2.b, above; and

e. All design materials used in the fabrication or assembly of the products referred to in paragraphs 2.a and 2.b, above.

3. This policy does not apply to the release of IA products to foreign governments and international organizations. Such release is governed separately by National Security Telecommunications and Information Systems Security Policy

[1] NSTISSI No. 4009, INFOSEC Glossary, Sept 2000, defines Information Assurance as information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

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

SECTION II – POLICY

4. U.S. Government activities are responsible for protecting U.S. Government classified and sensitive unclassified information. However, there may be certain circumstances when U.S. entities may also have a legitimate need to protect U.S. Government classified and sensitive unclassified information. In such situations, the U.S. Government may release IA products to these U.S. entities in accordance with the limitations set forth in paragraph 5, below.

5. Security policies and procedures applicable to any IA product that is released outside the federal government shall, in all cases, be consistent with established national IA doctrine and the specific requirements of this policy. In particular:

a. All individuals who are granted access to U.S. Government IA products must be U.S. citizens. Such access shall be controlled on a strict need-to-know basis and shall be granted only in conformance with procedures established for the particular type of IA products involved. Requests for release of IA products and services to U.S. individuals who are not U.S. citizens shall be processed as an exception to this policy.

b. Contracting for design, development, modification, production, or developmental testing of cryptographic equipment shall require prior approval of the Director, National Security Agency (NSA).

c. As a prior condition of release, IA products provided to U.S. entities shall be subsequently controlled in such a manner to prevent further dissemination outside the federal government. The same controls shall be in place to preclude the unauthorized transfer of technology contained therein.

d. Individuals who require access to U.S. classified cryptographic information must comply with applicable cryptographic access policies.

6. U.S. Government IA products may be released outside of the federal government provided the following criteria can be satisfied:

a. A valid need must exist for the individual or activity to:

(1) Install, maintain, or operate secure network or telecommunications equipment for the U.S. Government;

(2) Participate in the design, planning, production, training, installation, maintenance, operation, logistical support, integration, modification, testing, or study of IA products or techniques; or

(3) Communicate U.S. Government classified or sensitive unclassified information using secure network or telecommunication systems.

b. Individuals who are granted access to classified IA products must hold a final U.S. Government security clearance appropriate to the level of the classified material involved. Access to TOP SECRET material shall only be granted to individuals whose clearance is predicated on a favorable background investigation. Individuals who are granted an interim TOP SECRET clearance may not be granted access to IA products classified higher than SECRET.

c. All individuals who are granted access to IA products must receive a briefing regarding the unique nature of this material and must be made aware of their security responsibilities to properly safeguard and control any classified IA product.

d. All individuals who perform maintenance on hardware components of U.S. Government secure network or telecommunications equipment must receive formal NSA-approved training for the equipment or equipment family involved.

SECTION III – RESPONSIBILITIES

7. Heads of Federal Government departments and agencies are responsible for:

a. Making the decision to release IA products and services to U.S. entities after first determining that such release is in the best interest of the U.S. Government;

b. Ensuring that the criteria set forth in Section II of this policy are satisfied whenever IA products and services are released to U.S. entities;

c. Maintaining records of accountability for those U.S. entities to which that department or agency has authorized release of IA products and services;

d. Ensuring that those U.S. entities to which the IA products and services were released comply with established IA standards and doctrine, including all standards of security and quality assurance; and

e. Incorporating the criteria set forth in Section II of this policy into all contracts, agreements, or other appropriate documents whenever individuals who are not employees of the U.S. Government provide services identified in paragraph 6.a., above.

8. The Director, NSA, is responsible for:

a. Approving waivers to national-level requirements for the protection and control of IA products.

b. Providing assistance, when requested, to heads of other departments and agencies when determining whether to release IA products and services to U.S. entities.

SECTION IV – EXCEPTIONS

9. Exceptions to this policy may only be granted by the CNSS, except for those waivers that may be granted by the Director, NSA, as set forth in paragraph 8.a, above. Prior approval must be obtained in either case. Requests for CNSS approval of an exception, with appropriate justification, shall only be submitted by the head of a department or agency and forwarded to the CNSS through the Director, NSA, who shall provide appropriate recommendations for CNSS consideration. The checklist in the ANNEX should be used as a guide in preparing a request for exception.

Encl:
ANNEX A

ANNEX A

CHECKLIST FOR PREPARING REQUESTS FOR EXCEPTIONS TO THE PROVISIONS OF CNSS POLICY NO. 14

1. Identify the specific provision of CNSS Policy No. 14 for which an exception is required.

2. Identify the U.S. Government department or agency that is responsible for assuring the security and integrity of the IA operations/functions at the U.S. entity.

3. Identify the individual and/or activity requiring the exception, the citizenship and security clearance level of individual(s) involved, and the location(s) at which IA functions will be performed.

4. Identify the specific IA functions that are performed, the IA products to which the individual(s) has access, the number of individuals involved along with any training certification or statement of required training.

5. List the highest classification of the IA products to which the individual(s) will have access.

6. Indicate whether or not these individual(s) will be using CRYPTO-marked keying material that is held or used by any U.S. Government department or agency. If so, indicate whether unique operational keying material is needed by the entity(s) involved and provide a rationale for your decision.

7. Identify the inclusive dates for which the individual(s) will have access to the IA products as set forth in the contract, agreement, or sponsorship arrangement.

8. Indicate what compensatory administrative/security measures, if any, will be implemented in the event the request for exception is approved.