FACT SHEET

NSTISSP No. 11, Revised Fact Sheet
National Information Assurance Acquisition Policy

(Includes deferred compliance guidelines and procedures)

July 2003

Background

(1) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products was issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS), in January 2000 and revised in June 2003.

(2) The Committee was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems.

Introduction

(3) The technological advances and threats of the past decade have drastically changed the way we think about protecting our communications and communications systems. Three factors are of particular significance:

- The need for protection encompasses more than just confidentiality;

- Commercial Off-the-Shelf (COTS) security and security-enabled IA products are readily available as alternatives to traditional NSA-developed and produced communications security equipment (i.e., Government-Off-the Shelf (GOTS) products); and

- An increased and continuing recognition that the need for IA transcends more than just the traditional national security applications of the past.

(4) In the context of the second sub-bullet of paragraph (3), it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process, which will provide some assurances that these products perform as advertised. Accordingly, NSTISSP No. 11 has been developed as a means of addressing this problem for those products acquired for national security applications. NSTISSP No. 11 also rightfully points out that protection of systems encompasses more than just acquiring the right product. Once acquired, these products must be integrated properly and subject to an accreditation process, which will ensure total integrity of the information and systems to be protected.

Policy

(5) IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated GOTS or COTS IA and IA-enabled IT products. These products should provide for the availability of the systems, ensure the integrity and confidentiality of information, and ensure the authentication and non-repudiation of parties in electronic transactions.

(6) On 1 January 2001, preference was to be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which had been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

- The National Security Agency (NSA) /National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

- The NIST Federal Information Processing Standard (FIPS) validation program.

(7) Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets of paragraph (6).

(8) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(9) The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information

shall be limited to products which have been evaluated by NSA, or in accordance with NSA-approved processes.

(10) Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

(11) Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 (PDD-63), Critical Infrastructure Protection, dated 22 May 1998.

Responsibilities

(12) Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

Exemptions and Deferred Compliance

(13) COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

(14) While COTS IA and IA-enabled products (non-encryption based) have been developed, evaluated, and are available for acquisition and implementation on national security systems, it is recognized that these products do not cover the full range of potential user applications. Rapid technologic changes and the amount of time it takes to successfully complete a product evaluation also affect compliance with NSTISSP No. 11. Therefore, full and immediate compliance with NSTISSP No. 11 may not be possible for all acquisitions.

(15) No blanket or open-ended waivers to NSTISSP No. 11 will be authorized, but a Deferred Compliance Authorization (DCA)[1] may be granted on a case-by-case basis.

[1] A **Deferred Compliance Authorization** (DCA) is a formal approval by an authorized official to defer compliance with the requirements of a national IA policy for a specified period of time, normally not to exceed more than one calendar year.

Departments and agencies electing to pursue a DCA from the policy requirements of NSTISSP No. 11, shall use the following guidelines when determining whether a DCA is appropriate for a particular application and, if so, who has the authority for reviewing and approving a requested DCA.

Deferred Compliance Guidance

(16) The issuance of a DCA will apply only to environments not requiring the encryption of classified information. A DCA will not be submitted for encryption products. Encryption products for protecting classified information will be certified by NSA, and encryption products intended for protecting sensitive information will be certified in accordance with NIST FIPS 140-2.

(17) A DCA is applicable only to the acquisition of a specific COTS product for a specific application within the IT enterprise of an organization. It does not constitute blanket approval for future acquisitions of the same product and does not obviate the requirement for the requesting organization to obtain necessary certification and accreditation approval for the application or system in which the product will be used prior to operational use. A record of all DCAs will be included in certification and accreditation documentation.

(18) A DCA will be reviewed and approved only by the heads of federal departments or agencies, or major subordinate organizations with a department or agency (e.g., the Defense Intelligence Agency (DIA) within the Department of Defense). Heads of departments or agencies (or major subordinate organizations) may delegate their DCA review and approval authorities to a designee within their respective organizations. This normally would be the Chief Information Officer (CIO) or equivalent, or any other individual responsible for the security of the overall IT enterprise within that department or agency. Delegations of DCA authority must be formalized in writing and their currency maintained.

Deferred Compliance Procedures

(19) Those individuals or organizations (These could include IA/IT planners, designers, integrators, as well as acquisition entities.) responsible for IA within their respective departments or agencies will determine whether an evaluated product (or products) is available to satisfy a particular requirement.

(20) If an evaluated product is not available, DCA documentation will be prepared and submitted to the DCA approving authority. The DCA documentation must contain the following information:

- A description of the intended application and type of product needed;

- Details of why an evaluated product is not being procured (e.g., no products of this type have been evaluated, or an explanation as to why available evaluated products do not meet user's functional or security requirements);

- Product information, ideally the product's Security Target (i.e., the security claims being made by the vendor), and evidence (as documented by an appropriate department or agency testing facility) that the product's features and assurances are adequate for the intended application;

- The product quantity that is being acquired; and

- A statement that the requesting department or agency will, as a condition of purchase, require the product and its associated Security Target to be submitted for evaluation and validation to a Common Criteria Testing Laboratory accredited by the NSA/NIST NIAP Evaluation and Validation Program or a member nation recognized under the International Common Criteria for Information Technology Security Evaluation Security Mutual Recognition Arrangement.

(21) The Certifiers and Accreditors of systems that are relying on the security features and assurances of a product submitted and approved for a DCA should recognize that the security claims of the product have yet to be independently validated and therefore, should consider issuing Interim Approval to Operate (IATO) rather than Approval to Operate (ATO) for these systems.

(22) In the event an installed product fails to meet established validation and certification testing requirements during the period of the authorized DCA, it is recommended that Certifiers and Accreditors take steps to remove the product from national security systems falling under their purview. As with any security decision, the CIO (or equivalent authority) has the option of authorizing continued use of the failed product and accepting the risk of continued use, but should mandate follow-on actions that will ensure that the product is evaluated and validated for use on a national security system. Such "continue to operate" decisions should be formally documented and included in the overall system certification and accreditation documentation.

(23) The DCA approving authority will review and approve the DCA and submit the DCA documentation to the CNSS Secretariat through the Information Assurance Directorate (IAD) of the National Security Agency:

National Security Agency

ATTN: V1
Suite 6740
Ft. George G. Meade, MD 20755-6740

V1 may also be contacted via commercial phone at 410-545-4384 or fax at 410-854-6615.