FACT SHEET

NSTISSP No. 11

National Information Assurance Acquisition Policy

January 2000

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 is issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

(2) The NSTISSC 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 ways 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 information assurance (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.

NSTISSC Secretariat (I42) • National Security Agency • 9800 Savage Road STE 6716 • Ft Meade MD 20755-6716
(410) 854-6805 OR Toll Free 1-888-NSTISSC• UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

(4) In the context of the second of the above factors, 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, the attached policy has been developed as a means of addressing this problem for those products acquired for national security applications. The policy 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) Information Assurance (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 Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products should provide for the *availability* of the systems; ensure the *integrity* and *confidentiality* of information, and the *authentication* and *non-repudiation* of parties in electronic transactions.

(6) Effective 1 January 2001, preference shall 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 have 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) The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

(8) By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in paragraph (6), above, 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.

(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 the 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.

Responsibilities

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

Exemptions and Waivers

(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) Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the Director, National Security Agency (DIRNSA), ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary to support U.S. Government operations which are time-sensitive, or where U.S. lives may be at risk.