DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

Chief Information Officer

7 MAY 2002

MEMORANDUM FOR (SEE DISTRIBUTION LIST)

FROM: AF-CIO
1155 Air Force Pentagon
Washington DC 20330-1155

SUBJECT: AF-CIO Policy Memorandum 02-14; Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products

This memorandum implements National Telecommunications and Information Systems Security Policy (NSTISSP) Number 11, National Information Assurance Acquisition Policy, within the Air Force.

Effective immediately, all government personnel responsible for acquiring COTS/GOTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) will follow acquisition and implementation rules documented in Attachment 1. To maximize this policy's effectiveness, SAF/AQ will review and incorporate appropriate language modifications into the AF acquisition regulations/directives to ensure IT acquisitions are compliant with NSTISSP 11 within sixty days from the signature date of this memorandum. SAF/AQ is the lead for ensuring AF acquisition professionals are aware of this policy, have documented guidance on which to base their acquisition decisions, and comply with federal policies and processes for purchasing IA and IA-enabled IT products.

For affected intelligence systems, this policy does not alter or supersede existing authorities of the Director of Central Intelligence. Terms of reference for this policy are found at Attachment 2. My point of contact for this policy is Major Jack Kiesler, AF-CIO/PO, (703) 601-4044 (DSN: 329).

JOHN M. GILLIGAN
Chief Information Officer

Attachments:

1. Rules
2. Terms of reference
3. Distribution

Attachment 1

RULES

1. Per National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11, National Information Assurance Acquisition Policy, (Jan 2000), by 1 Jul 02, all government acquired COTS/GOTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) must be evaluated and validated, as appropriate IAW:

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

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

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

Note: Accredited commercial laboratories or NIST will conduct the evaluation/validation of COTS IA and IA-enabled IT products.

2. Per Department of Defense memorandum, components must continue to comply with the spirit and intent for the acquisition of all new IA or IA-enabled IT products, but with the following necessary qualifications as of July 1, 2002.

a. If an approved U.S. Government protection profile exists for a particular product type and there are evaluated and validated products available for use, then acquisition is restricted to those products.

b. If an approved U.S. Government protection profile exists for a particular product type and no evaluated and validated products exist, then acquisition documentation must contain requirements for evaluation and validation of the product to the approved protection profile.

c. If no U.S. Government protection profile exists for a particular product type, then acquisition documentation will require vendors to provide a security target that describes the security attributes of their product and have that product evaluated and validated or under contract to be evaluated and validated by a NIAP certified lab at a minimum of EAL2. When a U.S. Government protection profile is developed and released for that product type, the acquisition community will ensure that products of that particular type that are still in development are evaluated and validated to the new protection profile. Products that are in use under this option do not have to be re-evaluated when a protection profile is developed for that product type.

3. The National Information Assurance Partnership (NIAP) web site (http://niap.nist.gov/cc-scheme/ValidatedProducts.html) contains a current list of validated products.

4. GOTS IA and IA-enabled products acquired for systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products evaluated by NSA, or in accordance with NSA-approved processes.

5. COTS or GOTS IA and IA-enabled IT products acquired prior to this memo's effective dates are exempt from this policy; however, replacement upgrades and major modifications for those "exempt" products must comply.

6. The Committee on National Systems Security (CNSS), formerly known as National Security Telecommunications and Information System Security Committee (NSTISSC), may grant waivers to this policy on a case-by-case basis. Air Force waiver requests and justification must be submitted though HQ AFCA/WFP, Scott AFB IL, for evaluation and recommendation. The Information Assurance Sub-Architecture Council will then assess waiver requests and recommendations before forwarding to the Director, National Security Agency, who shall provide appropriate recommendations for CNSS consideration. While not mandatory, non-national security systems should consider the acquisition and implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems, which store, process, display or transmit sensitive or mission critical/essential information.

Attachment 2

TERMS OF REFERENCE

National Security System: Any telecommunications or information system operated by the US Government, the function, operation or use of which:

- Involves intelligence activities
- Involves cryptologic activities related to national security
- Involves command and control of military forces
- Involves equipment that is an integral part of a weapon or weapon system
- Is critical to the direct fulfillment of military or intelligence missions (to include logistics and resupply of military forces) and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, and personnel management applications)

COTS: "commercially available off-the-shelf item" that:

- Is a commercial item (as described in Title 41 U.S.C. 403(12)(A), implemented at FAR 2.101);
- Is sold in substantial quantities in the commercial marketplace;
- Is offered to the Government, without modification, in the same form in which it is sold in the commercial marketplace; and
- Does not include bulk cargo (as defined in Title 46 U.S.C. App. 1702), such as agricultural products and petroleum products.

Information Technology (IT):

- Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

- Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

- Notwithstanding subparagraphs (A) and (B), information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

IA IT Products: Products or technologies whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network interpolators, firewalls and intrusion detection devices.

IA-Enabled IT Products: Products or technologies whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

Attachment 3

DISTRIBUTION

ACC CIO/LG
AETC CIO/LG
AFMC CIO/LG/AQ
AFRC CIO/LG
AFSPC CIO/LG
AFSOC CIO/LG
AMC CIO/LG
ANG CIO/LG
PACAF CIO/LG
USAFE CIO/LG

CC:
AF/CVA
AF/DP
AF/IL
AF/RE
AF/XI
AF/SG
AF/ST
AF/TE
AF/XO
AF/XP
SAF/AA
SAF/AQ
SAF/FM
SAF/GC
AF-CIO/H
ESC/CC
AC2ISRC/CC