



**NATIONAL POLICY GOVERNING  
THE ACQUISITION OF  
INFORMATION ASSURANCE (IA)  
AND IA-ENABLED INFORMATION  
TECHNOLOGY PRODUCTS**



## CHAIR

### FOREWORD

1. The attached policy supersedes National Security Telecommunications and Information System Security Policy (NSTISSP) No. 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products,” dated January 2000 and revised in June 2003. CNSSP No. 11 clarifies the required evaluation processes applicable to Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) IA and IA-enabled IT products that are used on U.S. National Security Systems (NSS) to protect the information therein.

a. The National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) established the National Information Assurance Partnership (NIAP) program to implement and administer a process governing the testing and evaluation of COTS IA and IA-enabled IT products. The Director, NSA is responsible for implementing the NIAP as it applies to NSS to include approving processes for the evaluation of COTS products when they are to be used to protect information on NSS.

b. The Director, NSA, as the National Manager for NSS, is also directly responsible for establishing standards and criteria that GOTS IA and IT products must meet before they are used to protect NSS and the information therein.

2. Additional copies of this policy may be obtained by contacting the Secretariat or at the CNSS website: [www.cnss.gov](http://www.cnss.gov).

/s/

Teresa M. Takai

# NATIONAL POLICY GOVERNING THE ACQUISITION OF INFORMATION ASSURANCE (IA) AND IA-ENABLED IT PRODUCTS

	<u>SECTION</u>
<b>PURPOSE</b> .....	I
<b>AUTHORITY</b> .....	II
<b>SCOPE</b> .....	III
<b>POLICY</b> .....	IV
<b>RESPONSIBILITIES</b> .....	V
<b>DEFINITIONS</b> .....	VI
<b>REFERENCES</b> .....	VII

## SECTION I – PURPOSE

1. This policy establishes processes and procedures for the evaluation and acquisition of COTS and GOTS IA or IA-enabled IT products<sup>1</sup> to be used on U.S. NSS. The processes and procedures established in this policy will reduce the risk of compromising the NSS and the information contained therein and will:

- a. Ensure the security-related features of IA and IA-enabled IT products perform as claimed.
- b. Ensure the security evaluations of IA and IA-enabled IT products produce achievable, repeatable, and testable results.
- c. Promote cost effective and timely evaluations of IA and IA-enabled IT products.

## SECTION II – AUTHORITY

2. The authority to issue this instruction derives from National Security Directive 42, which outlines the roles and responsibilities for securing NSS consistent with applicable law; E.O. 12333, as amended; and other Presidential directives.

3. Nothing in this policy shall alter or supersede the authorities of the Director of National Intelligence.

---

<sup>1</sup> IA and IA-enabled products are those that have any mechanism providing for the availability of systems, ensuring the integrity and confidentiality of information, or ensuring the authentication and non-repudiation of parties in electronic transactions [source: Committee on National Security Systems Instruction No. 4009, “National Information Assurance Glossary,” April, 2010].

### **SECTION III – SCOPE**

4. This policy applies to all IA and IA-enabled IT products acquired for use by or on behalf of U.S. Government (USG) Departments and Agencies (D/A) to protect NSS and the information that resides therein<sup>2</sup>.

### **SECTION IV – POLICY**

5. All COTS IA and IA-enabled IT products acquired for use to protect information on NSS shall comply with the requirements of the NIAP program in accordance with NSA-approved processes and, where applicable, the requirements of the Federal Information Processing Standard (FIPS) Cryptographic validation program(s).

6. Layered COTS product solutions (e.g., selecting two or more IA and IA-enabled IT products) are preferred for use to protect information on NSS when these solutions are available and satisfy an organization's requirements.

7. GOTS products shall only be acquired or developed when an existing COTS IA and IA-enabled IT product solution is not available or is unable to satisfy an organization's requirements. All GOTS IA and IA-enabled IT products acquired for use to protect information on NSS shall be evaluated and certified by NSA, or in accordance with NSA-approved processes.

### **SECTION V – RESPONSIBILITIES**

8. Heads of U.S. Government Departments and Agencies shall:
- a. Ensure compliance with the requirements of this policy;
  - b. Select evaluated and validated COTS IA and IA-enabled IT products from the NIAP Product Compliant List (PCL)<sup>3</sup>;
  - c. Ensure GOTS IA and IA-enabled products acquired for use to protect information on NSS are evaluated by NSA, or in accordance with NSA-approved processes;
  - d. Work with the NIAP to identify and prioritize new commercial technologies requiring a NIAP-approved Protection Profile;

---

<sup>2</sup> This policy does not obviate requirements outlined in other CNSS policies or directives that may govern the acquisition of IT for NSS. Such policies are intended to be mutually supportive.

<sup>3</sup> The NIAP Product Compliant List can be found on the Internet at [http://www.niap-ccevs.org/CCEVS\\_Products/pcl.cfm](http://www.niap-ccevs.org/CCEVS_Products/pcl.cfm).

e. Participate in Protection Profile development whenever possible, in an open, public process in collaboration with industry, laboratories, academia, consortia, and standards groups to ensure maximum acceptance and usability;

f. Ensure layering and implementation of COTS IA and IA-enabled products acquired to protect classified information comply with NSA guidance<sup>4</sup>;

g. Ensure security categorization and controls as set forth in CNSS Instruction 1253, “*Security Categorization and Control Selection for National Security Systems*,” and National Institute of Standards and Technology Special Publication (NIST SP) 800-53 are met by the security solution in order to aid in the Authorizing Official’s (AO’s) approval of the implementation of the overall security solution; and

h. Contact the NSA Client Relationship Management Office<sup>5</sup> for assistance in selecting appropriate COTS/GOTS IA and IA-enabled IT products to implement a complete security solution.

9. NSA shall:

a. Provide approved evaluation processes for all COTS and GOTS IA and IA-enabled IT products to be used on or to protect NSS and the information contained therein;

b. Evaluate GOTS IA and GOTS IA-enabled IT products and certify those products that meet NSA-approved evaluation processes; and document and provide a security assessment for inclusion in the Security Authorization Package, (NIST SP 800-37 TASK 5-2);

c. Maintain a list of evaluated GOTS IA and IA-enabled IT products certified by NSA;

d. Assist USG D/A in determining an appropriate and complete security solution for a given environment;

e. Assist USG D/A in understanding and implementing the concept of a layered solution including the appropriate combinations and implementation of products in these solutions;

f. Assist USG D/A in selecting appropriate COTS products, including reducing risk for required technologies that have not been evaluated; and

g. Manage and staff the NIAP as it applies to NSS.

10. The Department of Commerce shall:

---

<sup>4</sup> Guidance for NSA’s Commercial Solutions for Classified process is located at [http://www.nsa.gov/ia/programs/csfc\\_program/index.shtml](http://www.nsa.gov/ia/programs/csfc_program/index.shtml)

<sup>5</sup> The NSA Client Relationship Management Office can be contacted at [www.nsa.gov/ia/contacts/index.shtml](http://www.nsa.gov/ia/contacts/index.shtml).

a. Accredite NIAP Common Criteria Test Laboratories (CCTLs) through the NIST National Voluntary Laboratory Accreditation Program (NVLAP), and

b. Manage and staff the NVLAP.

11. The NIAP shall:

a. Certify NIAP Common Criteria Test Laboratories (CCTLs);

b. Ensure evaluations and validations of COTS IA or IA-enabled IT products follow NSA-approved processes;

c. Develop, vet, and maintain NIAP-approved Protection Profiles, whenever possible, in an open, public process in collaboration with industry, laboratories, academia, consortia, and standards groups to ensure maximum acceptance and usability;

d. Publish NIAP-approved Protection Profiles that document security requirements for evaluating COTS IA and IA-enabled IT products in key technology areas (e.g., e.g., network devices, Internet Protocol Security (IPSec), Virtual Private Network (VPN) Gateway, VPN Client, Wireless Local Area Network (LAN) Access System, and Disk Encryption);

e. Collaborate with USG D/A and industry to prioritize the development of new Protection Profiles for additional COTS IA and IA-enabled IT products and, if no Protection Profile exists for a required technology, provide interim guidance;

f. Protect and promote COTS product innovation within the Protection Profile methodology, and through evaluation mechanisms;

g. Leverage industry standards to the maximum extent possible;

h. Map NIST Special Publication (SP) 800-53 security controls to Protection Profiles, as appropriate;

i. Maintain the NIAP PCL of COTS IA and IA-enabled IT products evaluated and validated pursuant to the NIAP program;

j. Ensure a managed transition from the current NIAP Validated Products List (VPL) to the NIAP PCL, whereby products from both lists may be used in the interim to satisfy the requirements of this policy;

k. Assist USG D/A in selecting appropriate COTS products from the NIAP PCL; and;

1. Maintain detailed implementation guidance for this policy within CNSS issuances and on the NIAP website at <http://www.niap-ccevs.org/>.

## **SECTION VI – DEFINITIONS**

12. The following definitions are provided to clarify the use of specific terms in the policy. All other terms used in this policy may be found in CNSS Instruction (CNSSI No. 4009), *National Information Assurance Glossary*:

a. Technical Community: Government/Industry/Academia partnerships formed around major technology areas to act like a standards body for the purpose of creating and maintaining Protection Profiles.

b. Protection Profile: A minimal, baseline set of requirements targeted at mitigating well defined and described threats. The term Protection Profile refers to NSA/NIAP requirements for a technology and does not imply or require the use of Common Criteria as the process for evaluating a product. Protection Profiles may be created by Technical Communities and will include:

- a set of technology-specific threats derived from operational knowledge and technical expertise;
- a set of core functional requirements necessary to mitigate those threats and establish a basic level of security for a particular technology; and,
- a collection of assurance activities tailored to the technology and functional requirements that are transparent, and produce achievable, repeatable, and testable results scoped such that they can be completed within a reasonable timeframe.

c. Layered COTS product solutions: Commercial IA and IA-enabled IT components used in layered solutions approved by NSA to protect information carried on NSSs.

## **SECTION VII – REFERENCES**

13. The following references apply:

a. National Security Directive (NSD) 42, “*National Policy for the Security of National Security Telecommunications and Information Systems*,” 5 July 1990.

b. Committee on National Security Systems Policy No. 15, “*National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*,” 1 October 2012.

c. Committee on National Security Systems Directive 502, “*National Directive on Security of National Security Systems*,” 16 December 2004.

d. Committee on National Security Systems Instruction No. 4009, “*National Information Assurance Glossary*,” 26 April, 2010.

e. Executive Order 12333, “United States Intelligence Activities,” as amended, 4 December 1981.

f. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “*Recommended Security Controls for Federal Information Systems and Organizations*,” Revised 30 April 2013.

g. CNSS Instruction 1253, “*Security Categorization and Control Selection for National Security Systems*,” 15 March 2012.