

CNSS Advisory Memorandum
Information Assurance 01-12
6 June 2012



Advisory Memorandum

NSA-Approved Commercial Solution

Guidance



NATIONAL MANAGER

FOREWORD

1. This Advisory Memorandum establishes new terminology and clarification for Commercial Solutions to protect National Security Systems (NSS) and the information they carry. A Commercial Solution, when properly implemented according to requirements and standards established and approved by the National Security Agency (NSA), may be used to protect classified and sensitive national security information.

2. This Advisory Memorandum shall be disseminated to all Government entities, contractors, and agents engaged in Information Assurance (IA) activities associated with NSS.

3. In addition to this Advisory Memorandum, further assistance with implementing the processes described herein is available to NSS owners and operators. The NSA is available to provide technical consulting to CNSS members to assist in solution development and threat mitigation. For further information, please contact the IAD Office of Client Engagement at (410) 854-4790.

4. Additional copies of this Advisory Memorandum may be obtained at www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/

DEBORA A. PLUNKETT

Advisory Memorandum
NSA-Approved Commercial Solution Guidance

SECTION I – APPLICABILITY

1. The authority to issue this Advisory Memorandum derives from National Security Directive No. 42, “*National Policy for the Security of National Security Telecommunications and Information Systems*,” dated 5 July 1990 (Reference a), which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives. This Memorandum applies to all Executive Departments and Agencies and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in Committee on National Security Systems (CNSS) Instruction 4009, “*National Information Assurance (IA) Glossary*,” dated 26 April 2010 (Reference b). Nothing in this Memorandum shall alter or supersede the authorities of the Director of National Intelligence.

SECTION II – BACKGROUND

2. Products and solutions that match the requirements of the term *Type-1 Product* are sought out by the Information Assurance (IA) community because they are “NSA approved” products or solutions. Reference b defines a *Type-1 Product* as: “Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed. Developed using established NSA business processes and containing NSA approved algorithms. Used to protect systems requiring the most stringent protection mechanisms.”

SECTION III – POLICY

3. The NSA will approve required configurations of Commercial Solutions for protecting classified and sensitive national security information. This solution shall be referred to as an *NSA-Approved Commercial Solution*. The Authorizing Official (AO), formerly known as the Designated Accrediting Authority (DAA), shall be responsible for ensuring that the implementation of the solution is in accordance with the documentation provided by the NSA.

4. The phrase *NSA-Approved Commercial Solution* shall be added to the next release of Reference b.

5. The NSA shall provide documentation relevant to the implementation of an NSA-Approved Commercial Solution (which may include a list of approved products, configuration guidance, and risk assessment). The department or agency that implements an NSA-Approved

Commercial Solution shall adhere to the NSA documentation and guidance provided, and the department or agency AO shall ensure that the solution is implemented correctly.

6. An NSA-Approved Commercial Solution when implemented shall be considered an IA component of a NSS and subject to security categorization and controls as set forth in CNSS Instruction 1253, “*Security Categorization and Control Selection for National Security Systems*,” (Reference c) and National Institute of Standards and Technology Special Publication (NIST SP) 800-53 (Reference d). The NSA shall identify the relevant CNSSI No. 1253 (Reference c) and NIST SP 800-53 (Reference d) controls that are met by the solution in order to aid in the AO’s approval of the implementation of the overall security solution.

7. An NSA-Approved Commercial Solution, whose implementation has been approved by the appropriate AO as being in accordance with NSA-provided documentation, may take the place of a certified Government-off-the-Shelf (GOTS) IA product to provide availability, confidentiality, integrity, authentication, non-repudiation and/or other security services necessary to protect classified and sensitive national security information. Nothing in this Memorandum is intended to supersede NSTISSP 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enables Information Technology (IT) Products,” dated June 2003, as amended.

SECTION IV – DEFINITIONS

8. The following definitions are provided to clarify the use of specific terms contained in this Advisory Memorandum. All other terms used in this issuance are defined in Reference b.

a. NSA-Approved Commercial Solution: The combination of multiple Commercial-Off-the-Shelf (COTS) IA products in a layered configuration that satisfies the security requirements of an operational use case, when properly implemented in accordance with NSA-approved requirements and standards.

b. Government Off-the-Shelf (GOTS): A software and/or hardware product that is developed by the technical staff of a government agency for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, but with funding and specification from the agency, and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the government.

SECTION V – REFERENCES

9. The following references apply to this Advisory Memorandum:

a. National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” dated 5 Jul 1990, as amended.

b. Committee on National Security Systems (CNSS) Instruction 4009, “National Information Assurance (IA) Glossary,” dated 26 April 2010.

c. Committee on National Security Systems (CNSS) Instruction 1253, “Security Categorization and Control Selection for National Security Systems,” dated 15 Mar 2012.

d. National Institute of Standards and Technology (NIST) Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” dated August 2009.

e. National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enables Information Technology (IT) Products,” dated June 2003.