Committee on National Security Systems

CNSS Policy No. 15
1 October 2012

National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems

Committee on National Security Systems

CHAIR

CNSSP No. 15

FOREWORD

1. This policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

2. In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Modern communications technology can provide global connectivity, but this technology is highly complex and presents a formidable challenge to achieving secure interoperability among information systems. The goal is to get the right information to the right users in a timely and secure manner to mitigate threats; respond to emergencies; or convey other sensitive, critical information. Achieving this goal requires cooperation across all levels of government, with industry, and with foreign partners and international organizations. This policy is focused on a critical component of this goal – providing the capability for information to be shared in an assured, secure, end-to-end manner.

3. The approach contained in this policy establishes use of a secure sharing suite using a standard suite of security protocols and cryptographic algorithms. The cryptographic protocols describe how to implement the cryptographic algorithms to achieve interoperability. The benefit of this approach is that protocols and algorithms will be widely available to governments and industry. The use of standardized protocols is the most efficient way to achieve interoperability. The selection of appropriate cryptographic algorithms and the associated parameters within those standards is necessary to enable secure interoperability among systems.

4. Additional copies of this policy may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

/s/
TERESA M. TAKAI

CNSS Secretariat (IE32) * National Security Agency * 9800 Savage Road * Suite 6716 * Ft Meade MD 20755-6716
Office: (410) 854-6805 * Unclassified FAX: (410) 854-6814
cnss@radium.ncsc.mil

Committee on National Security Systems

CNSSP No. 15

NATIONAL INFORMATION ASSURANCE POLICY ON THE USE OF PUBLIC STANDARDS FOR THE SECURE SHARING OF INFORMATION AMONG NATIONAL SECURITY SYSTEMS

SECTION I – APPLICABILITY AND SCOPE

1. This policy is applicable to all U.S. Government Departments and Agencies' acquisition of Information Assurance (IA) and IA-enabled Information Technology (IT) products incorporating cryptographic protocols and algorithms. It addresses IA and IA-enabled IT products that are required to satisfy the IA interoperability requirements associated with the protection of National Security Systems (NSS), as defined in 44 U.S.C. § 3542(b)(2), and the information that resides therein. This policy addresses the full range of IA services to include confidentiality, authentication, non-repudiation, integrity, and system availability. This policy supersedes the previous CNSS Policy No. 15, "National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems," dated March 2010.

SECTION II – REFERENCES

2. See ANNEX A.

SECTION III – DEFINITIONS

3. Definitions in Reference a. apply to this policy. Additional terms are defined in ANNEX D.

SECTION IV – POLICY

4. NSA-approved cryptography is required to protect NSS and the information that resides therein.

5. Widespread cryptographic interoperability among NSS requires:

a. The use of NSA-approved public standards-based security protocols. If mission unique requirements preclude the use of public standards-based security protocols, NSA-approved mission unique security protocols may be used; and

b. IA and IA-enabled IT products with integrated cryptography acquired by U.S. Government Departments and Agencies to protect NSS and the information that resides therein shall adhere to the following:

(1) After 1 October 2015, the appropriate Suite B cryptographic algorithms as listed in ANNEX B or a commensurate suite of NSA-approved cryptographic algorithms shall be included;

(2) Prior to 1 October 2015, the appropriate Suite B cryptographic algorithms as listed in ANNEX B and/or the appropriate legacy cryptographic algorithms as listed in ANNEX C, or a commensurate suite of NSA-approved cryptographic algorithms shall be included;

(3) Be compatible with NSA-approved public key and key management infrastructures as appropriate; and

(4) Successfully complete security protocol interoperability testing by an NSA-approved security protocol interoperability testing service.

6. Public key and key management infrastructures that support the use of IA and IA-enabled IT products that protect NSS must be approved by NSA and must comply with the appropriate provisions of Section IV, Paragraph 5.

7. To ensure interoperability, after 1 October 2015, all U.S. Government Departments and Agencies' infrastructures that provide products and services to support IA and IA-enabled IT products protecting NSS and the information that resides therein shall be able to support NSA-approved Suite B certificates and the Suite B cryptographic algorithms. A consolidated list of Secure Sharing Suite Compliant IA and IA-enabled IT products shall be promulgated in accordance with paragraph 11.d.

8. Achieving the requisite level of protection is dependent on more than just employing cryptographic algorithms. The quality of the implementation and supporting public key and key management infrastructures are equally important. Accordingly, IA and IA-enabled IT products acquired to protect NSS and the information that resides therein shall be evaluated or validated in accordance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 and all amendments thereto or successor policies (Reference b).

9. Subject to policy and guidance for non-NSS, U.S. Government Departments and Agencies should consider using this policy for applications where information sharing with a NSS might be required or where the protection of systems or information

may be critical to the conduct of organizational missions. This includes homeland security and critical infrastructure protection activities as addressed in Executive Orders 13228 (Reference c.), and 13231 (Reference d.), respectively.

SECTION V – RESPONSIBILITIES

10. Heads of U.S. Government Departments and Agencies shall:

a. Ensure compliance with this policy; and

b. Provide unfulfilled IA requirements for the protection of their NSS to the National Manager (Director, National Security Agency, ATTN: IA Directorate, IE).

11. The Director, National Security Agency shall:

a. Develop and promulgate interoperability profiles for NSA-approved public standards-based security protocols;

b. Develop interoperability procedures and tests, and integrate them into testing services;

c. Promulgate a list of security protocol interoperability testing services;

d. Promulgate a list of *Secure Sharing Suite Compliant* (see definition in Annex D) IA and IA-enabled IT products;

e. Provide advice, assistance, and guidance to U.S. Government Departments and Agencies in identifying protection requirements and selecting security protocols, cryptographic algorithms, and IA and IA-enabled IT products most appropriate to their needs for providing cryptographic interoperability and for protecting NSS and the information contained therein;

f. Develop and promulgate the Public Key Infrastructure (PKI) Suite B Certificate Policies (CPs) and profiles necessary to support IA and IA-enabled IT products that protect NSS;

g. Develop and promulgate Suite B key management guidance to support IA and IA-enabled IT products intended to protect NSS;

h. Review and approve all key management plans for IA and IA-enabled IT products intended to protect NSS;

i. Review and approve all public key and key management infrastructures that provide products or services to IA or IA-enabled IT products protecting NSS; and

j. Review and approve the key specifications for all keying material used by IA or IA-enabled products when protecting NSS.

ANNEX A

REFERENCES

a. Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," June 2006, or its successor.

b. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products", Revised June 2003, or its successor.

c. Executive Order 13228, "Homeland Security," 8 October 2001.

d. Executive Order 13231, "Critical Infrastructure Protection in the Information Age," 16 October 2001.

e. Federal Information Processing Standard Publication (FIPS PUB) 180-4, "Secure Hash Standard (SHS)," March 2012.

f. Federal Information Processing Standard Publication (FIPS PUB) 186-3, "Digital Signature Standard (DSS)," March 2009.

g. Federal Information Processing Standard Publication (FIPS PUB) 197, "Advanced Encryption Standard," November 2001.

h. NIST Special Publication (SP) 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," March 2007.

ANNEX B

Suite B – NIST cryptographic algorithms approved by NSA to protect National Security Systems and the information that resides therein.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197 (reference g.)	Use 128 bit keys to protect up to SECRET. Use 256 bit keys to protect up to TOP SECRET*
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A (reference h.)	Use Curve P-256[1] to protect up to SECRET. Use Curve P-384 to protect up to TOP SECRET.*
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use Curve P-256 to protect up to SECRET. Use Curve P-384 to protect up to TOP SECRET.*
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS PUB 180-4 (reference e.)	Use SHA-256 to protect up to SECRET. Use SHA-384 to protect up to TOP SECRET.*

* If an IA or IA-enabled IT product approved to protect up to SECRET information must interoperate at the SECRET and below level with IA or IA-enabled IT products that have been approved to protect up to TOP SECRET information, then it must include the capability to support the higher parameter modes.

[1] Reference f, Appendix 6, contains the specifications for Curve P-256 and Curve P-384.

ANNEX C

NIST-approved legacy cryptographic algorithms which may be used in place of Suite B cryptographic algorithms (ANNEX B) with identical functions.

Algorithm	Function	Specification	Parameters
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A (Reference h.)	Use 2048 bit modulus to protect up to SECRET.
Digital Signature Algorithm (DSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use 2048 bit modulus to protect up to SECRET.
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-3 (reference f.)	Use 2048 bit modulus to protect up to SECRET.

ANNEX D

DEFINITIONS OF SPECIALIZED TERMS

1. "Secure Sharing Suite (S3) Compliant" is defined as:

An IA or IA-enabled IT product that:

a. Uses NSA-approved public standards-based security protocols;

b. Includes (as selectable capabilities) the full set of Suite B cryptographic algorithms;

c. Has successfully completed NSA-approved security protocol interoperability testing; and

d. Has been evaluated or validated in accordance with NSTISSP No. 11.

2. "Suite B Compatible" is defined as:

An IA or IA-enabled IT product that:

a. Uses NSA-approved public standards-based security protocols. If none are available with the necessary functionality, then uses a NSA-approved security protocol;

b. Includes (as selectable capabilities) all of the Suite B cryptographic algorithms that are functionally supported by the NSA-approved security protocol(s); and

c. Has been evaluated or validated in accordance with NSTISSP No. 11.

3. "Security Protocol" is defined as:

An abstract or concrete protocol that performs security-related functions.