Committee on National Security Systems

CNSS Policy 15
20 October 2016

USE OF PUBLIC STANDARDS FOR SECURE INFORMATION SHARING

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION.

CHAIR

FOREWORD

1. This Policy specifies the use of public standards for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS). Based on analysis of the effect of quantum computing on Information Assurance (IA) and IA-enabled Information Technology (IT) products, the Policy updates the set of authorized algorithms to provide vendors and IT users more near-term flexibility in meeting their IA interoperability requirements. The set of authorized algorithms for long-term use on NSS will be specified in a subsequent update to this Policy.

2. Rapid and secure information sharing is essential to protect our Nation. Modern communications technology provides global connectivity but is highly complex and presents a formidable challenge to achieving secure interoperability among information systems. The goal is to transmit information in a timely and secure manner to mitigate threats, respond to emergencies, or convey other critical data. 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 sharing in an assured, end-to-end manner.

3. This Policy establishes a standard suite of cryptographic protocols and cryptographic algorithms. Standardized cryptographic protocols describe how to implement the cryptographic algorithms to achieve interoperability. This approach ensures protocols and algorithms will be widely available to government and industry.

4. This Policy supersedes Committee on National Security Systems (CNSS) Policy 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information among National Security Systems*, dated 1 October 2012, and CNSS Advisory Memorandum IA 02-15, *Use of Public Standards for the Secure Sharing of Information Among National Security Systems* (Reference a). Additional copies of this Policy may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

/s/

RICHARD A. HALE

USE OF PUBLIC STANDARDS FOR SECURE INFORMATION SHARING

SECTION I – PURPOSE

1. This Policy describes the requirements, roles, and responsibilities associated with the use of public cryptologic protocols and algorithms to protect NSS and the information residing therein, or transmitted between NSS. For the purposes of this Policy, the term "protecting NSS" will be interpreted as including the information contained therein, or transmitted between or among NSS.

SECTION II – AUTHORITY

2. The authority to issue this Policy is derived from National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (Reference b), which outlines the roles and responsibilities for securing NSS, consistent with Executive Order 12333, *United States Intelligence Activities*, as amended (Reference c), and other Presidential directives.

3. Nothing in this Policy alters or supersedes the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This Policy is applicable to all departments' and agencies' (D/As) acquisition of IA and IA-enabled IT products incorporating cryptographic protocols and algorithms. It addresses IA and IA-enabled IT products required to satisfy the IA requirements associated with the protection of NSS. This Policy applies to the full range of IA services, to including confidentiality, authentication, non-repudiation, integrity, and availability.

SECTION IV – POLICY

5. National Security Agency (NSA)-approved cryptography will be used to protect NSS.

6. To ensure widespread cryptographic interoperability among NSS, D/As will:

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

b. Acquire IA and IA-enabled IT products with integrated cryptography that:

(1) Uses appropriate public cryptographic algorithms as listed in Annex B or a commensurate suite of NSA-approved cryptographic algorithms; and

(2) Is compatible with NSA-approved public key and key management infrastructures as appropriate.

7. 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 6, above.

8. To ensure interoperability, all D/As' infrastructures that provide products and services to support IA and IA-enabled IT products protecting NSS will be able to support NSA-approved certificates for the public cryptographic algorithms identified in Annex B.

9. 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 shall be evaluated or validated in accordance with CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products* (Reference d).

10. Subject to policy and guidance for non-NSS, D/As should consider using this Policy for applications where information sharing with an NSS is possible or where the protection of systems or information may be critical to the conduct of organizational missions. This would include homeland security and critical infrastructure protection activities as addressed in Executive Order 13228, *Establishing the Office of Homeland Security and the Homeland Security Council* (Reference e), and Executive Order 13231, *Critical Infrastructure Protection in the Information Age* (Reference f), respectively.

11. NSA may, upon a decision by the National Manager and notification provided to the CNSS, update the list of approved cryptographic algorithms in Annex B without requiring a reissuance of this Policy.

SECTION V – RESPONSIBILITIES

12. Heads of U.S. Government D/As will:

a. Ensure compliance with this Policy; and

b. Provide unfulfilled IA requirements related to this Policy to the National Manager (Director, National Security Agency, ATTN: IA Engagement).

13. The Director, NSA will, for IA and IA-enabled IT products that protect NSS:

a. Provide advice, assistance, and guidance to D/As in identifying protection requirements and selecting security protocols, cryptographic algorithms, and products most appropriate to their needs for providing cryptographic interoperability;

b. Develop and promulgate the Public Key Infrastructure (PKI) and appropriate public Certificate Policies and profiles;

c. Develop and promulgate key management guidance;

d. Review and approve all key management plans;

e. Review and approve all public key and key management infrastructures that provide products or services; and

f. Review and approve the key specifications for all keying material.

SECTION VI – DEFINITIONS

14. Definitions in CNSS Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary* (Reference g) apply to this Policy.

SECTION VII – REFERENCES

15. References for this Policy are contained in Annex A.

ANNEX A

REFERENCES

a) CNSS Advisory Memorandum 02-15, *Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, July 2015 (hereby superseded).

b) National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, 5 July 1990.

c) Executive Order 12333, *United States Intelligence Activities*, 4 December 1981, as amended.

d) CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*, 10 June 2013.

e) Executive Order 13228, *Establishing the Office of Homeland Security and the Homeland Security Council*, 8 October 2001.

f) Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, 16 October 2001.

g) CNSS Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015.

h) Federal Information Processing Standard Publication (FIPS PUB) 197, *Advanced Encryption Standard (AES)*, 26 November 2001.

i) NIST Special Publication (SP) 800-56A Rev 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013.

j) FIPS PUB 186-4, *Digital Signature Standard (DSS)*, July 2013.

k) FIPS PUB 180-4, *Secure Hash Standard (SHS)*, August 2015.

l) Internet Engineering Task Force (IETF) Request for Comments (RFC) 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*, May 2003.

m) NIST SP 800-56B Rev 1, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, September 2014.

ANNEX B

NSA-APPROVED COMMERCIAL NATIONAL SECURITY ALGORITHM (CNSA) SUITE

1. The following table contains NIST cryptographic algorithms approved by NSA to protect NSS.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197 (Reference i)	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 Rev 2 (Reference j)	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	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 l)	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526 (Reference m)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key-establishment	NIST SP 800-56B Rev 1 (Reference n)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	Minimum 3072 bit-modulus to protect up to TOP SECRET.

2. Additional Information:

   a. PKI systems are in the midst of transitioning from SHA-1 to SHA-256 and currently employ 2048-bit RSA. Similarly, certain equipment that is not scheduled for replacement at this time cannot use moduli larger than 2048-bits for Diffie-Hellman Key exchanges. Alternatively, a change in course to deploy elliptic curve cryptography (ECC) may add additional cost to the transition without providing the long-life benefit originally presumed due to the potential advent of quantum computing.

   b. For these reasons, deployments using commercial technology solely for the protection of UNCLASSIFIED NSS data or for community of interest separation may continue to use RSA and Diffie-Hellman at the 2048 bit level and SHA-256 in the near term. D/As planning to deploy ECC with P-256 likely require a further change (e.g., to P-384) before quantum-resistant algorithms reach sufficient market penetration. The intent is to avoid multiple hops wherever possible; therefore, D/As planning to deploy ECC with curves other than P-384 to protect UNCLASSIFIED NSS or to provide community of interest separation must consult with NSA before proceeding.

ANNEX C

ACRONYMS

AES	Advanced Encryption Standard
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
D/A	Department/Agency
DH	Diffie-Hellman
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
IA	Information Assurance
IETF	Internet Engineering Task Force
IT	Information Technology
NSA	National Security Agency
NSS	National Security Systems
PKI	Public Key Infrastructure
PUB	Publication
RFC	Request for Comments
SHA	Secure Hash Algorithm
SP	Special Publication