Committee on National Security Systems

CNSS Advisory Memorandum
Information Assurance 02-15
July 2015

ADVISORY MEMORANDUM

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

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems (CNSS) is issuing this Advisory Memorandum to inform agencies of updated National Security Agency (NSA) guidance associated with the use of public algorithms to protect National Security Systems (NSS).

2. This Advisory expands on the guidance contained in CNSS Policy No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems* (Reference a). Based on analysis of the effect of quantum computing on Information Assurance (IA) and IA-enabled Information Technology (IT) products, the policy's set of authorized algorithms is expanded to provide vendors and IT users more near-term flexibility in meeting their IA interoperability requirements. The purpose behind this additional flexibility is to avoid vendors and customers making two major transitions in a relatively short timeframe, as we anticipate a need to shift to quantum-resistant cryptography in the near future.

3. For further information, please contact the NSA Information Assurance Directorate's Office of Client Engagement at (410) 854-4790.

4. This advisory is available from the CNSS Secretariat, as noted below, or the CNSS website: www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/

WAYNE M. MURPHY

ADVISORY MEMORANDUM
USE OF PUBLIC STANDARDS FOR THE SECURE SHARING OF INFORMATION AMONG NATIONAL SECURITY SYSTEMS

SECTION I – PURPOSE

1. This Advisory outlines the public algorithms which should be used to protect NSS. The use of approved public cryptographic algorithms encourages widespread information sharing while still maintaining security. Rapid and secure information sharing is important to protect our Nation, its citizens and its interests.

SECTION II – AUTHORITY

2. The authority to issue this Advisory derives 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 applicable law, Executive Order 12333 (Reference c), as amended, and other Presidential directives.

3. Nothing in this Advisory should be interpreted as altering or superseding the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This Advisory is applicable to all U.S. Government Departments and Agencies' (D/As) acquisition of IA and IA-enabled IT products incorporating NSA-approved public cryptographic protocols and algorithms which are required to satisfy the IA requirements associated with the protection of NSS, as defined in 44 U.S.C. § 3542(b)(2), and the information that resides therein. It does not apply to classified Government Off-the-Shelf (GOTS) developments. This Advisory applies to the full range of IA services to include confidentiality, authentication, non-repudiation, integrity, and system availability. This Advisory serves as an expansion of the allowed algorithms defined in Reference a.

SECTION IV – BACKGROUND

5. Reference a provides guidance on the use of public standards for cryptographic protocol and algorithm interoperability to protect NSS. Based on analysis of the effect of quantum computing on IA and IA-enabled IT products, the set of authorized algorithms outlined in Reference a needs to be expanded to provide vendors and IT users more near-term flexibility in meeting their IA interoperability requirements.

6. This Advisory establishes use of a standard suite of NSA-approved public cryptographic 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 government D/As 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.

SECTION V – GUIDANCE

7. As stated in Reference a, NSA-approved cryptography is required to protect NSS and the information that resides therein.

8. 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. The following public algorithms should be used to protect IA and IA-enabled IT products with integrated cryptography acquired by U.S. Government D/As to protect NSS and the information that resides therein shall adhere to the following:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197	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	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	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	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP

			SECRET
RSA	Asymmetric algorithm used for key establishment	FIPS SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

9. Large scale deployments of 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 is not able to use moduli larger than 2048-bits for Diffie-Hellman Key exchanges. A change in course to deploy elliptic curve cryptography (ECC) appears to add additional cost to the transition without providing the long-life benefit originally presumed due to the potential advent of quantum computing. 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. Those who deploy or plan to deploy ECC with P-256 likely require a further change (e.g. to P-384) before quantum-resistant algorithms reach sufficient market penetration. It is our intent to avoid such multiple hops wherever possible; therefore, we ask that anyone deploying or planning to deploy ECC with curves other than P-384 consult with NSA before proceeding.

10. Reference a will be updated to incorporate this guidance. U.S. Government D/As should conform to the guidance above until an update to Reference a is complete.

SECTION VI – REFERENCES

11. References for this advisory are listed in ANNEX A.

Enclosures:
ANNEX A – References
ANNEX B – Acronyms

ANNEX A

REFERENCES

a. 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 1 October 2012.

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

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

ANNEX B

ACRONYMS

Advanced Encryption Standard	AES
Committee on National Security Systems	CNSS
Departments and Agencies	D/As
Diffie-Hellman	DH
Elliptic Curve Cryptography	ECC
Elliptic Curve Diffie-Hellman	ECDH
Elliptic Curve Digital Signature Algorithm	ECDSA
Federal Information Processing Standards	FIPS
Government Off-the-Shelf	GOTS
Information Assurance	IA
Internet Engineering Task Force	IETF
Information Technology	IT
National Institute of Science and Technology	NIST
National Security Agency	NSA
National Security Systems	NSS
Request for Comment	RFC
Rivest-Shamir-Adelman	RSA
Secure Hash Algorithm	SHA