Commercial National Security Algorithm Suite

The Commercial National Security Algorithm Suite (CNSA Suite) will provide new algorithms for those customers who are looking for mitigations to perform, replacing the current Suite B algorithms.

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

View related Algorithm Guidance documents.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.

For those vendors and partners that have already transitioned to Suite B, we recognize that this took a great deal of effort on your part, and we thank you for your efforts. We look forward to your continued support as we work together to improve information security for National Security customers against the threat of a quantum computer being developed. Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy.

It is important to note that we aren't asking vendors to stop implementing the Suite B algorithms and we aren't asking our national security customers to stop using these algorithms. Rather, we want to give more flexibility to vendors and our customers in the present as we prepare for a quantum safe future. Where elliptic curve protocols are to be used, we prefer Suite B standards be used to the fullest extent possible as they have a long history of security evaluation and time tested implementation that newer proposals do not yet have.

Guidance

For those customers who are looking for mitigations to perform while the new algorithm suite is developed and implemented into products, there are several things they can do. First, it is prudent to use larger key sizes in algorithms (see the table below) in many systems (especially, smaller scale systems). Additionally, IAD customers using layered commercial solutions to protect classified national security information with a long intelligence life should begin implementing a layer of quantum resistant protection. Such protection may be implemented today through the use of large symmetric keys and specific secure protocol standards.

For example, CSfC deployments involving an IKE/IPsec layer may use RFC 2409-conformant implementations of the IKE standard (IKEv1) together with large, high-entropy, pre-shared keys and the AES-256 encryption algorithm. RFC 2409 is the only version of the IKE standard that leverages symmetric pre-shared keys in a manner that may achieve quantum resistant confidentiality. Additionally, MACsec key agreement as specified in IEEE 802.1X-2010, and the RFC 4279 TLS specification provide further options for implementing quantum resistant security measures today. These options also involve key agreement schemes that leverage large symmetric pre-shared keys.

With respect to IAD customers using large, unclassified PKI systems, remaining at 112 bits of security (i.e. 2048-bit RSA) may be preferable (or sometimes necessary due to budget constraints) for the near-term in anticipation of deploying quantum resistant asymmetric algorithms upon their first availability.

Related Items

1 Algorithms to Support the Evolution of Information Assurance Needs
2 CNSA Suite and Quantum Computing FAQ
3 Commercial Solutions for Classified (CSfC) Tri-fold
4 Mathematical routines for the NIST prime elliptic curves
5 Ransomware - Locky

Have Questions?

Frequently Asked Questions
Site Index
E-mail: Cybersecurity Requirements

During the current transition phase, the public algorithms in the following table should be used to protect 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.

Transition Algorithms

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	NIST 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.

CNSS Advisory Memo

A CNSS Advisory Memo is or will soon be available on the **CNSS website**. This CNSS Advisory Memo will serve as the official interim guidance to NSS customers until a revision to *CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among National Security Systems*, is published codifying the increased near-term algorithm flexibility described above.

Export Control

Certain commercial IA and IA-enabled IT products that contain cryptography and the technical data regarding them are subject to Federal Government export controls. Export of products that implement NIST specifications that define public domain cryptographic algorithms or associated technical data must comply with Federal Government regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Information about export regulations is available at the Bureau of Industry & Security.

Commercial Solutions for Classified (CSfC) Program

The NSA Commercial Solutions for Classified (CSfC) Program has been established to enable commercial products to be used in layered solutions protecting classified NSS data. This will provide the ability to securely communicate using a layered commercial solution based on public cryptography and secure protocol standards. Visit the Commercial Solutions for Classified Program site for more information including the current CSfC Components List.

Point of Contact

For questions about Suite B and Cryptography Today contact the National Cryptographic Solutions Management Office (NCSMO) at (410) 854-8577.

Last Reviewed: 19 August 2015