Commercial National Security Algorithm (CNSA) Suite

Rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms are vital tools that contribute to our national security and help address the need for secure, interoperable communications. The National Security Agency (NSA) is responsible for approving solutions for protecting National Security Systems (NSS). Many systems in the NSS community are planned over decade timescales, have very long lifetimes after deployment, and are used to protect data that requires confidentiality for years beyond that.

Since 2005, a specific set of elliptical curve based algorithms, the CNSA cryptographic algorithms as specified by the National Institute of Standards and Technology (NIST), have been used by NSA in solutions approved for protecting classified and unclassified NSS. After observing the past decade of progress in quantum computing research, NSA endorses the increasing consensus that quantum computers will pose a threat in the future and that protocols using public key algorithms in the market place today will eventually need to be addressed. Given the longevity and unique nature of NSS and the costs of converting our existing public key based infrastructure to new algorithms, it is prudent to reconsider our strategic approach to the protection of data on NSS now.

To ensure the confidentiality of our customers' long life data, NSA is planning for an upcoming transition to quantum resistant algorithms and encouraging the design and analysis of quantum resistant public key algorithms. NSA plans to support NIST and other external standards bodies in developing standards for quantum resistant cryptography. In 2015, NSA announced a revised set of cryptographic algorithms that can be used to protect NSS while the algorithms that would be part of a quantum resistant suite are developed. For symmetric algorithms, options exist today that will be sufficient well into the future and beyond the development of a quantum computer. In the public key space, the intent is to give more flexibility to vendors and our customers in the present as we prepare for a quantum safe future.

Commercial cryptography approved to protect NSS systems up to the TOP SECRET level

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Block cipher used for information protection	FIPS Pub 197	Use 256 bit keys
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384
Elliptical Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384
Secure Hash Algorithm (SHA)	Used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384
Diffie-Hellman (DH) Key Exchange	Algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus
RSA	Algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072-bit modulus