# The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

## Sections



## Background

**Q: To whom are these requirements addressed?**

A. These are mainly addressed to the following audiences:

- National Security System (NSS) owners/operators, who need to know the requirements for their systems
- Vendors, who need to know what to implement to meet NSS requirements

NSA is not using these requirements to dictate or recommend to any other entity outside of NSS and the Defense Industrial Base (DIB) what algorithms they should use, although NSA recognizes that interoperability requirements or other interests may lead to scenarios where these recommendations are used by a larger community.

**Q: What is a quantum computer, and how is it different from the computers we use today?**

A: In place of ordinary bits used by today's computers, quantum computers use "qubits" that behave in surprising ways, efficiently performing certain mathematical algorithms exponentially faster than a classical computer. Small examples of quantum computers have been built.

**Q: What is a "cryptanalytically relevant quantum computer" (CRQC)?**

A: Also written as "cryptographically relevant quantum computer," CRQC describes quantum computers that are capable of attacking real world cryptographic systems. Whether the "C" indicates "cryptanalytically" or "cryptographically" is a matter of writer's preference, as the two terms are essentially equivalent in this context. This term distinguishes a CRQC from any other "quantum computer" technologies used in other settings without the performance metrics required to attack real world cryptographic systems.

**Q: What is the threat if a CRQC were developed?**

A: A CRQC, if built, would be capable of undermining the widely deployed public-key algorithms currently used for asymmetric key exchanges and digital signatures with potentially devastating impact to systems. National security systems (NSS) use public-key cryptography as a critical component to protect the confidentiality, integrity, and authenticity of national security information.

**Q: Can I continue to use larger sizes of RSA or ECC to address the threat?**

A: No. RSA and Elliptic Curve Cryptography are the main algorithms that need to be replaced to achieve quantum resistance.

**Q: What is "quantum-resistant" or "post-quantum" cryptography?**

A: "Quantum-resistant" (QR), "quantum-safe," and "post-quantum" (PQ) cryptography are all terms used to describe cryptographic algorithms that can be run on computers today and are believed to be resistant to cryptanalytic attacks from both classical and quantum computers.

**Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?**

A: CNSA 2.0 is the suite of QR algorithms approved for eventual NSS use. The following table lists the algorithms and their functions, specifications, and parameters.

*Table: Commercial National Security Algorithm Suite 2.0*

| Algorithm | Function | Specification | Parameters |
|---|---|---|---|
| Advanced Encryption Standard (AES) | Symmetric block cipher for information protection | FIPS PUB 197 | Use 256-bit keys for all classification levels. |
| ML-KEM (aka CRYSTALS-Kyber) | Asymmetric algorithm for key establishment | FIPS PUB 203 | Use Category 5 parameter, ML-KEM-1024, for all classification levels. |
| ML-DSA (aka CRYSTALS-Dilithium) | Asymmetric algorithm for digital signatures in any use case, including signing firmware and software | FIPS PUB 204 | Use Category 5 parameter, ML-DSA-87, for all classification levels. |
| Secure Hash Algorithm (SHA) | Algorithm for computing a condensed representation of information | FIPS PUB 180-4 | Use SHA-384 or SHA-512 for all classification levels. |
| Leighton-Micali Signature (LMS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. LMS SHA-256/192 is recommended. |
| Xtended Merkle Signature Scheme (XMSS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. |

## CNSA 2.0

**Q: Where should CNSA 2.0 algorithms be used?**

A: CNSA 2.0 algorithms will be required for all products that employ public-standard algorithms in NSS, whether a future design or currently fielded. Any usage of Suite B or CNSA 1.0 algorithms will be required to transition to CNSA 2.0 usage. The Timeframe

section of this FAQ and the Advisory Memorandum have transition timeframe information. More details will be released on an ongoing basis as industry adjusts to the new technology.

**Q: How did NSA choose the CNSA 2.0 algorithms?**

A: NSA chose algorithms from among those selected for standardization by the National Institute of Standards and Technology (NIST), the U.S. Government lead for commercial algorithm approval. NSA believes they offer optimal performance for given NSS security requirements.

**Q: How strong does NSA believe CNSA 2.0 algorithms are?**

A: NSA performed its own analysis of CNSA 2.0 algorithms and considers them appropriate for long-term use in protecting the varied missions of U.S. NSS.

**Q: Does NSA intend to produce implementation guidance for CNSA 2.0 similar to the IETF RFCs[1] produced for CNSA 1.0?**

A: NSA will provide implementation guidance for CNSA 2.0 algorithms, and is working with the IETF to produce them through the RFC series. RFCs detail protocol options in addition to algorithm choices, and NSA expects to provide similar protocol guidance regardless of algorithm selection.

**Q: For whom is this guidance intended?**

A: NSA makes CNSA 2.0 requirements, anticipated timing, and this related FAQ widely available to assist NSS owners and operators in their transition planning and to inform industry of NSS requirements.

**Q: Does CNSA 2.0 apply to fielded equipment?**

A: Even NSS systems that are in current use will need to be upgraded in a timely fashion unless the system received a waiver through the approved process. This is in

[1] Internet Engineering Task Force Requests for Comments.

agreement with National Security Memorandums (NSMs) 8[2] and 10[3] as well as CNSSP 11 and CNSSP 15.

**Q: What policies should I follow to meet NSS algorithm requirements?**

A: High-grade equipment will follow the guidance in CJCSN 6510[4] and CNSSAM 01-07-NSM[5]. Commercial equipment will follow CNSA 1.0 until the transition mandated by CNSSP 15[6], expected to occur sometime between 2025 and 2030, depending on equipment type. In accordance with NSM-10 and CNSSP-11, QR algorithms should be implemented in NSS mission systems as National Information Assurance Partnership (NIAP) validated products or in accordance with other implementation-specific guidance. Typically, this will include, but not be limited to, requiring modules be validated by the NIST Cryptographic Module Validation Program (CMVP).

**Q: Where can I learn more about hash-based signatures?**

A: Refer to NIST standardized stateful hash-based signatures in NIST SP 800-208[7]. This standard also provides references to other technical documentation on the topic. NSA recommends using Federal Information Processing Standards (FIPS)-validated LMS or XMSS hash-based signatures to protect NSS in the specialized scenarios outlined in the standard—e.g., for firmware signing and software signing. NSA's preferred parameter set is Section 4.2, LMS with SHA-256/192.

**Q: Can I use HSS or XMSSMT from NIST SP 800-208?**

A: From NIST SP 800-208, NSA has only approved LMS and XMSS for use in NSS. The multitree algorithms HSS and XMSSMT are not allowed.

[2] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 19 January 2022.

[3] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022.

[4] Chairman of the Joint Chiefs of Staff Notice 6510, Information Assurance Cryptographic Device Modernization Requirements, August 2019.

[5] Committee on National Security Systems Advisory Memorandum 01-07-NSM, Cryptographic Equipment Modernization Planning, 20 March 2022.

[6] Committee on National Security Systems Policy 15, Use of Public Standards for Secure Information Sharing.

[7] NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes.

**Q: Can I use SLH-DSA (aka SPHINCS+) to sign software?**

A: While SLH-DSA is hash-based, it is not part of CNSA and is not approved for any use in NSS.

**Q: I'm going to adopt LMS or XMSS for software/firmware validation. Which components need to be validated, and how? If my hardware security module (HSM) is not FIPS-validated, can I get a waiver?**

A: Signature verification is expected to be performed by code that has been validated by NIST's Cryptographic Algorithm Validation Program (CAVP). It is expected that signed code may be received from a variety of sources (signers). If your product is only validating signatures, CAVP testing is all that is required.

Code sources (signers) that are NSS are required to produce signatures according to NIST SP 800-208, which requires hardware validated by NIST's Cryptographic Module Validation Program (CMVP), or via other NSA guidance. Waivers will not be granted for this.

While code sources (signers) that are not NSS are not subject to CNSA requirements, they are expected to use code that meets the same development and operational quality as the validated code, that is, code that can pass CAVP testing.

Note: to avoid weakening the security of these signatures, one should implement signing and state management in hardware, such as an HSM. Backup flows, which may involve transferring keys between modules, must prevent state re-use.

**Q: As a commercial vendor, how do I know if my NIST SP 800-208 implementation meets CNSA 2.0?**

A: NIAP validates products against its published Protection Profiles, which will start including quantum-resistant signatures in line with our published transition timelines. For commercial vendors, we do not anticipate NIAP Protection Profiles will perform signature generation within the Target of Evaluation (TOE) boundary, only signature verification. As signature generation is the component of LMS/XMSS that requires state management, if only signature verification is being performed, only CAVP validation (not CMVP) will be expected for such products.

**Q: Why are signatures for software- and firmware-signing listed separately?**

A: The reasons for choosing separate algorithms for software- and firmware-signing are as follows:

- NIST has standardized the algorithms in NIST SP 800-208 already and has CAVP validation available, while other post-quantum signatures are not yet standardized,
- This signature use-case is more urgent,
- This selection places hash-based algorithms, with their substantial history of cryptanalysis, in a use case where their well-described potential performance issues have minimal impact. In particular, this usage coincides well with the requirement for keeping track of state—that is, how many times a given public key was used in signing software or firmware when deploying these signatures.

**Q: Why are firmware signatures more urgent?**

A: In many firmware-signing cases the validation algorithm is not easily updated. Thus, firmware-signing algorithms are frequently locked in for the life of a system. Even in systems that are designed for extensibility and cryptographic agility, a quantum-resistant root of trust may be required in the firmware years before the rest of the system upgrades to quantum-resistance. NSA prioritizes this in our timelines to avoid unexpected costs and security issues later in our transition.

**Q: Can I use SHA-3 as a hash?**

A: No, neither SHA-3 nor SHAKE are approved for use in CNSA as a hash algorithm. While NSA allows any parameter set of LMS, including some that call SHA-3 as a function, NSA has not approved SHA-3 as a hash algorithm. Its use is strictly limited to those cases where it is prescribed by the standard describing an NSA-approved algorithm, such as LMS within NIST SP 800-208.

The SHA-2 selections are sufficient for security, and their ubiquity in the commercial world ensures interoperability. Using SHA-3 or SHAKE outside those narrowly defined applications where it is called as a function significantly increases the interoperability testing burden and breaks many use cases for CNSA 2.0.

**Q: Where can I learn more about lattice-based key encapsulation mechanisms (KEMs) and digital signatures?**

A: NIST announced it would standardize lattice-based KEMs and digital signatures. NIST's post-quantum standardization page includes reports from previous rounds of the standardization effort. These reports include summaries of the cryptography under consideration and many references.

**Q: Why did NSA choose ML-DSA over FN-DSA (aka Falcon)?**

A: For NSS, NSA agrees with NIST: ML-DSA is preferred, as FN-DSA seems more susceptible to implementation errors that may affect security. As NIST has prioritized standardizing ML-DSA, it will likely be available sooner.

**Q: Can I use ML-DSA for firmware or software signing?**

A: At this time LMS and XMSS are the only approved digital signing algorithms which have finished standards and validation paths. Firmware roots of trust are a critical component to upgrade and NSA expects this to be implemented for some long-lived signatures in 2025, before validated ML-DSA is widely available. NSA prefers to see this transition begin now rather than wait for ML-DSA due to the long timeframes involved in moving from small components and/or early designs to completed products.

ML-DSA is approved for all signing use cases and when it is available (i.e., standardized and validated) it may be reasonable for some software/firmware signing use cases. For example, when a user's software signing strategy requires more signatures than can be reasonably used with a single LMS or XMSS key, or in software development environments with a distributed signing system, it would be reasonable to use ML-DSA.

**Q: Will NSA add more selections to CNSA in the future?**

A: NSA does not currently plan to add future NIST post quantum standards to CNSA. Circumstances could change in ways we do not currently foresee, but adding more algorithms generally makes interoperability more complex (although admittedly less so for algorithms for software and firmware signing).

**Q: What if my solution uses hash functions other than SHA-384 or SHA-512?**

A: SHA-384 remains approved in the newest CNSA Suite, as NSA believes it provides sufficient security for NSS. Designers often prefer to use SHA-512 for performance reasons. This is now supported by CNSA 2.0; however, customers need to be certain that using SHA-512 does not lead to interoperability issues.

Where NSA has approved an algorithm or cryptographic application that incorporates a truncated hash value or other NIST-approved hash function (e.g. SHA-3) as part of its design, using those hash functions is acceptable within the scope of the algorithm or cryptographic application. General purpose use of such hash functions is not approved at this time.

Just as SHA-512 was added to CNSA, NSA may in the future add another NIST algorithm if it achieves ubiquity in a key area of the ecosystem, satisfies our independent security requirements, and is unlikely to interfere with interoperability.

**Q: How is CNSA 2.0 implementation enforced in NSS?**

A: Authorizing officials will be reporting regularly on adoption in accordance with NSM-10. It is important they use the tools and resources available to ensure all systems that use cryptography for security (including software update mechanisms) implement CNSA 2.0 algorithms. Report any deviations to NSA in accordance with NSM-10 processes.

**Q: Can a commercial product be used in my NSS that runs cryptography other than in CNSA 2.0?**

A: If a commercial product does not use CNSA 2.0 algorithms, it is not allowed to be used to protect NSS unless it is approved through the waiver process. CNSA 2.0 relies on NIST standardized algorithms, which have been widely vetted as quantum resistant, and other algorithms should not be employed. Further, CNSSP-11 requires that commercial products used in NSS be NIAP validated, and this validation will generally require CNSA 2.0 compliance.

**Q: When should deployment of CNSA 2.0 algorithms in mission systems begin?**

A: When validated products become available they should be deployed in mission systems. Meanwhile, NSA encourages responsible testing in vendor and government

research environments now to understand the effects of deployment of the new algorithms on particular systems given the increased sizes used in these algorithms.

## Timeframe

**Q: What timeframe information can NSA provide for adoption of CNSA 2.0?**

A: NSA intends that all NSS will be quantum-resistant by 2035, in accordance with the goal espoused in NSM-10. NSA relies upon NIST-approved commercial cryptography for commercial solutions. After NIST has finalized the standards associated with CNSA 2.0, NSA will update CNSSP 15.

New cryptographic developments will be required to support CNSA 2.0 algorithms as an option once appropriate standards for the given technology are in place. All appropriate system components should be configured to prefer CNSA 2.0 algorithms. As products mature, those components should be configured to accept only CNSA 2.0 algorithms.

NSA will provide guidance and updated protection profiles as industry develops the appropriate standards because product lines may develop at different speeds. CNSA 1.0 algorithms will continue to be used until current solutions can operate in a CNSA 2.0 mode. NSA's current view on timing is as follows:

- **Software- and firmware-signing:** begin transitioning immediately, support and prefer CNSA 2.0 by 2025 where available, *exclusively* use CNSA 2.0 by 2030.
- **Web browsers/servers and cloud services**: support and prefer CNSA 2.0 by 2025, *exclusively*[8] use CNSA 2.0 by 2033.
- **Traditional networking equipment (e.g., virtual private networks, routers):** support and prefer CNSA 2.0 by 2026, *exclusively* use CNSA 2.0 by 2030.
- **Operating systems**: support and prefer CNSA 2.0 by 2027, *exclusively* use CNSA 2.0 by 2033.
- **Niche equipment (e.g., constrained devices, large public-key infrastructure systems)**: support and prefer CNSA 2.0 by 2030, *exclusively* use CNSA 2.0 by 2033.
- **Custom applications and legacy equipment**: update or replace by 2033.

[8] Even though NSA may allow or require hybrid solutions due to protocol standards, product availability, or interoperability requirements CNSA 2.0 algorithms will become mandatory to select at the given date, and selecting CNSA 1.0 algorithms alone will no longer be approved.

**Q: What is the timeline for new deployments?**

A: NIAP and the Commercial Solutions for Classified (CSfC) program will update their profiles and requirements in accordance with industry adoption. NSA intends an aggressive timeframe for adoption (see the bullets above) and requests industry support.

**Q: What is the timeline for transitioning fielded equipment?**

A: As industry adopts CNSA 2.0 algorithms, NSA will require transition of fielded equipment to CNSA 2.0 as well. In some circumstances, this may require a hardware refresh. NSA encourages NSS owners and operators to plan for this.

Cryptographic agility is necessary to accomplish this transition in a timely manner; even equipment purchased before support is mandated should have sufficient memory and processing power when possible to run new algorithms, as well as capacity for future algorithms and protocols so that any future enhancements can be included via a software update.

**Q: When will NIST standards become completed/finalized?**

A: This question is best addressed to NIST. See NIST's Post-Quantum Cryptography Standardization project page for more information.

**Q: When will IETF RFCs for implementing NSA's algorithms be available?**

A: IETF and other standards development organizations (SDO) are independent bodies. NSA is working with IETF and other SDOs to produce RFCs and other documentation with the appropriate level of security and implementation analysis that these important standards are due. NSA encourages CNSA 2.0 adoption in standards and deployment in vendor products.

## Preparation

**Q: What can developers and programs do to prepare for a future quantum-resistant algorithm suite?**

A: AES-256, SHA-384, SHA-512, and the NIST hash-based signatures listed in NIST SP 800-208 are considered safe against attack by a large quantum computer. Developers should deploy these algorithms today. They should also begin implementing

the other quantum-resistant algorithms NIST and NSA chose and provide feedback about any issues they discover. NSS owners and operators should test implementations of algorithms in lab networks to prepare for the transition.

**Q: How do I begin to transition to a quantum-resistant system?**

A: The CNSA 1.0 Suite continues to represent the interim strategy as the commercial space transitions to the algorithms in CNSA 2.0. Following forthcoming NSA guidance and NIST efforts, including NIST's forthcoming 1800-38 series, will best position NSS owners and operators to make this transition.

**Q: Is there a quantum-resistant public-key algorithm that commercial vendors should adopt today?**

A: NSA encourages vendors to use CNSA 2.0 approved hash-based signatures for software- and firmware-signing. NSA does not approve using pre-standardized or non-FIPS-validated CNSA 2.0 algorithms (even in hybrid modes) for NSS missions. However, NSA does recommend limited use of pre-standardized or non-FIPS-validated CNSA 2.0 algorithms and modules in research settings to prepare for the transition. NSA requests vendors begin preparing to implement CNSA 2.0 algorithms so they are primed to provide products soon after NIST completes standardization.

## CNSSP 15

**Q: What is CNSSP 15?**

A: Committee on National Security Systems Policy 15 (CNSSP 15) specifies commercial cryptographic algorithms for protecting NSS, in conjunction with other CNSS- and NSA-documented processes. Originally, it specified "NSA Suite B," and then it was revised to specify the CNSA 1.0 Suite in CNSSP 15 Annex B. It will include CNSA 2.0 algorithms as NIST completes standardizing the selections from Round 3 of the standardization process. Further details about CNSS are at www.cnss.gov.

**Q: What will happen with CNSSP 15?**

A: The October 2016 update to CNSSP 15 made three significant changes, as follows:

1. It replaced the previous requirement to transition systems to “Suite B” standards, specifying a larger selection of algorithms (i.e., CNSA) to allow extended use of existing solutions while post-quantum standards are developed.

2. It consolidated the two security levels of Suite B into a single set of requirements for use at all levels.

3. Finally, while the previous version of CNSSP 15 focused exclusively on classified information, the updated policy applies to all NSS, both classified and unclassified.

NSA plans to update algorithms in CNSSP 15 with the CNSA 2.0 suite of algorithms as the recent cybersecurity advisory, “Announcing the Commercial National Security Algorithm Suite 2.0,” notes, and to deprecate CNSA 1.0 algorithms in the next version. NSA plans to keep the other previous changes as they are, having a single set of requirements for both unclassified and all levels of classified NSS.

**Q: How does CNSSP 15 relate to CNSSI 1253, NIST SP 800-53, and the RMF process?**

A: CNSS Instruction 1253[9] mandates using the Risk Management Framework (RMF) as documented in NIST SP 800-39[10] and NIST SP 800-53[11] in managing National Security Information Systems. NIST SP 800-53 includes security controls (e.g., SC-12) that relate to cryptography. NSS requires the “NSA Approved” selection. Unless NSA states otherwise, the “NSA Approved” cryptography selection includes CNSA 1.0 algorithm requirements as well as all other relevant NSA guidance on product validation and operation.

**Q: How should the broader government community understand CNSSP 15 requirements?**

A: NSA establishes NSS requirements. Often these systems require protection for long periods against targeted efforts sophisticated and well-resourced adversaries conduct in

[9] Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems.

[10] NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

[11] NIST Special Publication 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations.

potential wartime settings. NIST establishes cryptographic standards for other government systems.

NSA selected the algorithms in CNSSP 15 from those chosen by NIST in order to satisfy both NSA requirements for NSS and to simplify implementation and interoperability by aligning with NIST standards for general government use. If you are uncertain whether NSS requirements apply to a specific system, contact NSA for assistance. Also see NIST SP 800-59[12].

## Quantum alternatives

**Q: Can I mitigate the quantum threat by using a pre-shared key?**

A: Many commercial protocols allow a pre-shared key option that may mitigate the quantum threat, and some allow the combination of pre-shared and asymmetric keys in the same negotiation. However, this issue can be complex. Customers who wish to explore this option should contact NSA or follow guidance the CSfC program provides.

**Q: Will quantum computers affect non-public-key (i.e., symmetric) algorithms?**

A: Quantum computing techniques are generally considered much less effective against symmetric algorithms than against current widely used public-key algorithms. While public-key cryptography requires fundamental design changes, symmetric algorithms are considered secure, provided the key size is sufficiently large. CNSA 2.0 symmetric algorithms, which essentially are the same as their CNSA 1.0 counterparts, are quantum-resistant.

**Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?**

A: NSA does not know when there will be a CRQC. Expert assessments disagree significantly about timing. Because NSS often have very long lifecycles, NSA must produce requirements today for systems that will be used many decades in the future. Consequently, the data these systems protect will still require cryptographic protection for decades after these systems are at end of life. There is growing research in the area

[12] NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.

of quantum computing, and enough progress that NSA must act now to protect NSS by providing the requirements for the transition to CNSA 2.0.

**Q: What is quantum key distribution (QKD)?**

A: The field of quantum cryptography involves specialized hardware using the physics of quantum mechanics to protect the confidentiality of sensitive information. The most common example today uses quantum physics to distribute keys for use in a traditional symmetric algorithm, known as “quantum key distribution” or QKD. This technology exists today and is distinct from the quantum computing technology that might one day attack cryptographic algorithms. The sole function of QKD is to distribute keys between users. Hence, it is only one part of a cryptographic system.

**Q: Can I use a QKD system to protect my national security system from a quantum computer?**

A: No. The technology involved is of significant scientific interest, but it only addresses some security threats and requires significant engineering modifications to NSS communications systems. NSA does not generally consider QKD a practical security solution for protecting NSS. NSS owners should not use or research QKD at this time without consulting NSA directly. For specific questions, NSS owners can contact NSA.

**Q: What is a quantum random number generator (quantum RNG)?**

A: Quantum random number generators are hardware random number generators that use specific quantum effects to generate nondeterministic randomness. The decision on which RNG is appropriate in a specific scenario depends on many factors. In addition, any properly certified/approved RNG should be acceptable if you implement it within the constraints of that approval.

## Commercial Solutions for Classified (CSfC) and National Information Assurance Partnership (NIAP)

**Q: Can I use any CNSA 1.0- or CNSA 2.0-capable product(s) in my NSS without going through NIAP/CSfC?**

A: No, CNSSP 11 states that all commercial-off-the-shelf information assurance (IA) and IA-enabled information technology products acquired to protect information on NSS shall comply with NIAP program requirements according to NSA-approved processes

and, where applicable, the requirements of FIPS cryptographic validation programs. Furthermore, CNSSP 7 states that a CSfC solution may protect NSS provided the appropriate Authorizing Official approved it and registration with NSA's CSfC Program Management Office showed it compliant with an NSA-provided Capability Package.

**Q: I have long data life concerns and want to adopt CSfC solutions. How can I ensure my communications and data remain secure against an adversary with a quantum computer?**

A: Some CSfC solutions may be implemented today using symmetric, pre-shared keys that protect against the long-term quantum computing threat. NSA considers using pre-shared symmetric keys in a standards-compliant fashion a better near-term post quantum solution than implementing experimental post-quantum asymmetric algorithms possibly incompatible with NIST standards. Eventually, NSA will provide capability packages—to coincide with commercial technological development—to implement CNSA 2.0 algorithms.

For details, contact the CSfC program office.

## Future cryptographic algorithms

**Q: What algorithms should I use for other areas of cryptography (e.g., Blockchain, Private Information Retrieval, Identity Based Encryption)?**

A: NSA wants to know about potential use cases for any of the innovative cryptography listed below (or other similar cryptographic innovation). CNSSP 15 mandates using public standards, while allowing exceptions for additional NSA-approved options when needed. Neither NSA nor NIST has produced standards for these areas, and NSA has not issued any general approval for using these technologies.

Many of these topics involve novel security properties requiring further scrutiny. NSS owners should consult NSA before using any cryptography that CNSA 1.0 or CNSA 2.0 and other published guidance do not specify. In particular, the following have no generally approved solutions:

- Distributed ledgers or blockchains
- Private information retrieval (PIR)
- Private set intersection (PSI)
- Identity-based encryption (IBE)

- Attribute-based encryption (ABE)
- Homomorphic encryption (HE)
- Group signatures
- Ring signatures
- Searchable encryption
- Threshold signatures

**Q: I have a novel cryptographic solution. How do I get my solution "NSA Approved?"**

A: NSA has programs for certifying solutions built to protect classified information. This certification process applies to developments intended specifically for government use or control. NSA also participates in efforts such as NIAP and runs the Commercial Solutions for Classified program, both of which require strictly complying with traditional cryptographic standards and designs.

NSA does not accept direct requests from commercial vendors to validate their products or offer a general use vendor certification for novel cryptographic solutions. If an NSS customer believes they have a mission need to use cryptography beyond what is currently available, they should engage with NSA directly to discuss their unique situation.

**Q: Will NSA be adopting the standards from NIST's Lightweight Cryptography effort?**

A: NSA does not intend to add the ciphers resulting from NIST's Lightweight Cryptography effort to CNSA. The Lightweight Cryptography effort resulted in the selection of symmetric primitives based on the Ascon family. Their targeted security is substantially less than AES-256, rendering them generally unsuitable for NSS use cases. If CNSA 2.0 algorithms do not meet mission system performance requirements, early consultation with NSA is required.

## Hybrids

**Q: What is a hybrid cryptographic solution?**

A: A hybrid solution for a protocol is one using multiple algorithms to perform the same function, such as key agreement or authentication. The solution uses algorithms in a way that requires an attacker to break each one to compromise system security. Hybrid

solutions can consist of many traditional or QR algorithms. “Component algorithms” are individual algorithms used in a hybrid solution.

**Q: What is NSA’s position on the use of hybrid solutions?**

A: NSA has confidence in CNSA 2.0 algorithms and will not require NSS developers to use hybrid certified products for security purposes. Product availability and interoperability requirements may lead to adopting hybrid solutions.

NSA recognizes that some standards may require using hybrid-like constructions to accommodate the larger sizes of CRQC algorithms and will work with industry on the best options for implementation.

**Q: What complications can using a hybrid solution introduce?**

A: Hybrids add complexity to protocols, as designers need to incorporate additional negotiation and error handling and implementers need to modify API’s and testing.

Rather than ease the transition to quantum resistance, hybrid deployments introduce additional interoperability concerns, now that all algorithms plus the method of hybridization must be features common to all parties to a communication. Similarly, hybrid deployments add a second transition later as users eventually move away from classical algorithms in the future.

At the same time, hybrid solutions make the implementations more complex, so one must balance the risk of flaws in an increasingly complex implementation with the risk of a cryptanalytic breakthrough. Because more security products fail due to implementation or configuration errors than failures in their underlying cryptographic algorithms, spending limited resources to add cryptographic complexity can at times weaken security rather than improve it.

Where NSA recognizes a need to support a hybrid solution, extensive work will be performed to ensure that it can be safely implemented, including engineering to a high degree of robustness, and facilitation to a straightforward transition to QR-only solutions.

**Q: Is there an example where NSA will recommend hybrid solutions?**

A: Due to technical details of how the IKEv2 protocol operates with post-quantum cryptography's larger messages, it is not possible to directly replace the CNSA 1.0 public key algorithms with their CNSA 2,0 counterparts in IKEv2. Because implementations will already require the use of new messages and code to support post-quantum extensions, NSA anticipates keeping the initial CNSA 1.0 algorithms as a hybrid layer together with CNSA 2.0 algorithms for key establishment within IKEv2 indefinitely.

**Q: Should one use a hybrid or other non-standardized QR solution while waiting for a final NIST post-quantum standard?**

A: Do not use a hybrid or other non-standardized QR solution on NSS mission systems except for those exceptions NSA specifically recommends to meet standardization or interoperability requirements. NSA encourages limited purchase and use for research and planning, but only to prepare for transitioning to a CNSA 2.0 Suite. Because NSA is confident that CNSA 2.0 algorithms will sufficiently protect NSS, it does not require a hybrid solution for security purposes.

Using non-standard solutions entails a significant risk of establishing incompatible solutions. Using a hybrid solution that involves a symmetric key in accordance with established standards (e.g., RFC 8446, RFC 8784) may be appropriate, but key management complexity generally restricts this to specialized applications.

## Further information

**Q: Where can I get more information?**

A: For CSfC-specific questions, customers should contact the Commercial Solutions for Classified Program Management Office at CSfC@nsa.gov.

Other specific questions from NSS users may be addressed via e-mail to NSACryptoToday@nsa.gov or through normal business channels.

***Disclaimer of endorsement***

manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## *Purpose*

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

## *Contact*

Cybersecurity Report Inquiries and Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov