



Commercial National Security Algorithm Suite 2.0 and Quantum Computing Frequently Asked Questions

These frequently asked questions (FAQ) and answers clarify Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) requirements for National Security Systems (NSS) and recommend guidance for the Department of War (DoW) and the Defense Industrial Base (DIB). This information may be useful more generally, especially for those who interact with NSS, DoW, or DIB systems.

Sections

- [Background](#)
- [CNSA 2.0](#)
- [Timeframe](#)
- [CNSSP 15 and NSM-10](#)
- [Quantum alternatives](#)
- [Commercial Solutions for Classified \(CSfC\) and National Information Assurance Partnership \(NIAP\)](#)
- [Future cryptographic algorithms](#)
- [Hybrids and composites](#)
- [Additional information](#)



Table of Contents

Sections	1
Table of Contents	2
Background	6
Q: Who is the intended audience for these requirements?	6
Q: What is a quantum computer, and how is it different from the computers we use today?	6
Q: What is a “cryptanalytically relevant quantum computer” (CRQC)?	6
Q: How would a CRQC pose a threat?	6
Q: Can I continue to use larger sizes of RSA or Elliptic Curve Cryptography (ECC) to address the threat?	7
Q: What is “quantum-resistant” or “post-quantum” cryptography?	7
Q: What do “full QR” and “partial QR” mean?	7
Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?	7
CNSA 2.0	8
Q: Where should CNSA 2.0 algorithms be used?	8
Q: How did NSA choose the CNSA 2.0 algorithms?	8
Q: How strong are CNSA 2.0 algorithms according to NSA?	8
Q: Does NSA intend to produce guidance for CNSA 2.0, similar to the Internet Engineering Task Force (IETF) Requests for Comments (RFCs) produced for CNSA 1.0?	9
Q: Who is the intended audience for this guidance?	9
Q: Does CNSA 2.0 apply to fielded equipment?	9
Q: What policies should I follow to meet NSS algorithm requirements?	9
Q: What should I do if NSA has not published guidance about how to use these algorithms in my application?	10
Q: What is the difference between ML-KEM and CRYSTALS-Kyber, or between ML-DSA and CRYSTALS-Dilithium?	10
Q: When should I use hash-based signatures, and which should I use?	11
Q: Can I use HSS or XMSSMT from NIST SP 800-208?	11
Q: Can I use SLH-DSA (aka SPHINCS+) to sign software?	11



Q: I'm going to adopt LMS or XMSS for software/firmware validation for NSS. Which components need to be validated, and how? If my hardware security module (HSM) is not FIPS-validated, can I get a waiver?	11
Q: As a commercial vendor, how do I know if my NIST SP 800-208 implementation meets CNSA 2.0?	12
Q: Why are signatures for software- and firmware-signing listed separately from signing other information?	12
Q: Why are firmware signatures more urgent?	13
Q: Under what circumstances is SHA-3 available for use?.....	13
Q: Can I use SHA-3 in protocols that validate my virtual machines (VMs)?	13
Q: Can I use SHA-3 as a hash?	14
Q: Can I use SHA-3 and SHA-256 for self-contained non-hash purposes, specifically as a pseudo-random function in deterministic random bit generators (DRBGs) and key derivation functions (KDFs), or as an alternative to XOR for combining submasks?	14
Q: Are there any plans to add SHA-3/SHAKE to the "General Purpose Algorithms" section of CNSA?	14
Q: Where can I learn more about lattice-based key encapsulation mechanisms (KEMs) and digital signatures?	15
Q: Why did NSA choose ML-DSA over FN-DSA (aka Falcon)?	15
Q: Can I use ML-DSA for firmware or software signing?	15
Q: Is HashML-DSA, also known as the pre-hash mode of ML-DSA, allowed in CNSA 2.0?.....	15
Q: Will NSA add more selections to CNSA in the future?	16
Q: How is CNSA 2.0 implementation enforced in NSS?	16
Q: Can a commercial product be used in my NSS that runs cryptography other than in CNSA 2.0?.....	16
Q: When should CNSA 2.0 algorithms begin deployment in mission systems?	16
Timeframe	17
Q: What is NSA's recommended timeframe for CNSA 2.0 adoption?	17
Q: Will I need to transition all my algorithms at once to CNSA 2.0?	17
Q: What is the timeline for new deployments?.....	18



Q: I am a vendor whose product was NIAP-certified before the QR requirements were finalized. What is my product's status?	18
Q: If no CNSA 2.0 compliant products meeting my needs are available on January 1, 2027, is it acceptable to purchase an updateable product and deploy the CNSA 2.0 options later?	18
Q: What is the timeline for transitioning fielded equipment?	18
Q: When will IETF RFCs containing guidance on configurations for CNSA 2.0 compliant protocols be available?	19
CNSSP 15 and NSM-10	19
Q: What is National Security Memorandum (NSM) 10?	19
Q: What is CNSSP 15?	19
Q: What changes are in the CNSSP 15 update?	20
Q: As an NSS owner, when will my quantum-resistant transition be completed according to the reporting requirements under NSM-10?	20
Q: How does CNSSP 15 relate to CNSSI 1253, NIST SP 800-53, and the RMF process?	21
Q: How should the broader government community understand CNSSP 15 requirements?	21
Q: Are there other broad government policies to transition to QR algorithms?	21
Q: How does the recent Executive Order 14412 impact your guidance?	22
Quantum alternatives	22
Q: Can I mitigate the quantum threat to NSS by using a pre-shared key?	22
Q: Will quantum computers affect non-public-key (i.e., symmetric) algorithms?	23
Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?	23
Q: I just read a news report or scientific paper asserting quantum computers are coming soon. Is NSA's timeline correct?	23
Q: Given the threat, is the NSS community moving aggressively enough to mitigate the impact of an early CRQC?	24
Q: What is quantum key distribution (QKD)?	24
Q: Can I use a QKD system to protect my national security system from a quantum computer?	24
Q: What is a quantum random number generator?	24



Commercial Solutions for Classified (CSfC) and National Information Assurance Partnership (NIAP)	25
Q: Can I use any CNSA-capable product(s) in my NSS without going through NIAP/CSfC?.....	25
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?.....	25
Future cryptographic algorithms	26
Q: What algorithms should I use for other areas of cryptography (e.g., Blockchain, Private Information Retrieval, Identity Based Encryption)?.....	26
Q: I have a novel cryptographic solution. How do I get my solution “NSA Approved?”	26
Q: Will NSA be adopting the standards from NIST’s Lightweight Cryptography effort?	27
Q: Will NSA be adopting the standards from NIST’s Post-Quantum Signature On-Ramp effort?	27
Q: What does this mean for cryptocurrencies?	27
Hybrids and composites	27
Q: What is a hybrid or composite cryptographic solution?	27
Q: What is NSA’s position on the use of hybrid solutions?	28
Q: If I use a hybrid solution in my NSS, am I quantum resistant?	28
Q: What complications do hybrid solutions introduce?	28
Q: Is there an example where NSA will recommend hybrid solutions?.....	29
Q: I don’t want to tear out my quantum-vulnerable root of trust today. Do I need to use a composite signature?.....	29
Q: Should one use a hybrid or other non-standardized QR solution while waiting for a final post-quantum protocol standard for any specific technologies?	30
Additional information.....	30
Q: Where can I get more information?.....	30



Background

Q: Who is the intended audience for these requirements?

A. The requirements are primarily for:

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

NSA does not mandate requirements on any other entity outside of NSS. However, these requirements may serve as guidance for entities outside of NSS, especially where interoperability requirements or other interests may lead to these recommendations being used by a broader 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 different ways, efficiently performing certain mathematical algorithms exponentially faster than a classical computer. Small quantum computers are commercially accessible today.

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

A: Also written as "cryptographically relevant quantum computer," a CRQC describes a quantum computer 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: How would a CRQC pose a threat?

A: If built, a CRQC would be capable of undermining the widely deployed public-key algorithms currently used for asymmetric key exchanges and digital signatures with potentially devastating impacts to 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 Elliptic Curve Cryptography (ECC) to address the threat?

A: No. RSA and ECC 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 to describe cryptographic algorithms that can run on computers today and are believed to be resistant to cryptanalytic attacks from both classical and quantum computers. In contrast to QR algorithms, a CRQC will undermine “quantum-vulnerable” algorithms’ security properties.

Q: What do "full QR" and "partial QR" mean?

A: In current systems, quantum-vulnerable algorithms perform many cryptographic services. These include confidentiality, authentication, and identity management. As systems upgrade, some of these services have seen faster QR solution deployment than others. Many systems offer quantum-resistant encryption before they offer quantum-resistant identity management, so they will sometimes advertise as "partially QR." A system is considered "fully QR" when all the cryptographic services it provides are resistant to cryptanalytic attacks by a CRQC.

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 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
General Purpose Algorithms			
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 for all classification levels.



Algorithm	Function	Specification	Parameters
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.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS) & Xtended Merkle Signature Scheme (XMSS)	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.
Secure Hash Algorithm 3 (SHA-3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

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 for a future design or currently fielded. Any usage of Suite B or CNSA 1.0 algorithms are required to transition to CNSA 2.0. The [Timeframe](#) section of this FAQ and CNSSP 15 provide 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 standardized 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 NSS security requirements.

Q: How strong are CNSA 2.0 algorithms according to NSA?

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 guidance for CNSA 2.0, similar to the Internet Engineering Task Force (IETF) Requests for Comments (RFCs) produced for CNSA 1.0?

A: NSA will provide direction for using CNSA 2.0 algorithms securely in a variety of use cases and is working with the IETF to produce informational guides for protocol deployment through the RFC series. RFCs detail protocol options, in addition to algorithm choices, and NSA expects to provide protocol guidance to ensure smooth and secure operation with CNSA 2.0 algorithms.

Q: Who is the intended audience for this guidance?

A: These FAQs primarily can assist NSS owners and operators in their transition planning, and inform industry and vendors of NSS requirements. This guidance is also useful for those seeking to interoperate with NSS, or for any organization seeking similar robust security and interoperability requirements.

Q: Does CNSA 2.0 apply to fielded equipment?

A: Even NSS currently in use need to upgrade in a timely fashion unless they receive a waiver through the approved process. This is consistent with [National Security Presidential Memorandum \(NSPM\) 12](#)¹ and [National Security Memorandum \(NSM\) 10](#),² as well as CNSSP 11³ and CNSSP 15.⁴

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

A: High-grade equipment will follow the guidance in [CJCSN 6510](#)⁵ and [CNSSAM 01-07-NSM](#).⁶ Commercial equipment will follow [CNSSP 15](#), which mandates transition no later than 2030; specific deadlines are dependent 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

¹ National Policy for the Cybersecurity of National Security Systems, 12 June 2026.

² National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022.

³ Committee on National Security Systems Policy 11, National Policy Governing the Acquisition of Cybersecurity and Cybersecurity-enabled Information Technology Products and Services.

⁴ Committee on National Security Systems Policy 15, Use of Public Standards for Secure Information Sharing.

⁵ Chairman of the Joint Chiefs of Staff Notice 6510, Information Assurance Cryptographic Device Modernization Requirements, August 2019.

⁶ Committee on National Security Systems Advisory Memorandum 01-07-NSM, Cryptographic Equipment Modernization Planning, 20 March 2022.



accordance with other implementation-specific guidance. Typically, this will include, but not be limited to, requiring modules validated by the NIST Cryptographic Module Validation Program (CMVP).

NIAP has updated nearly all Protection Profiles (PPs) to add QR options. In 2027, NIAP will no longer accept products for certification that have not started their quantum transition, and will begin archiving certificates of products that do not conform to these PPs. Even though products may have been acquired at the time that they had valid NIAP certificates, and usually archiving NIAP certifications does not require discontinuing use of the products, NSM-10 and CNSSP 15 do not allow continued use of quantum-vulnerable algorithms and require products to upgrade in accordance with the timelines set forth unless the system receives a waiver through the approved process.

Q: What should I do if NSA has not published guidance about how to use these algorithms in my application?

A: While the CNSA 2.0 RFCs published through the IETF, NIAP PPs, and other guidance documents released by NSA cover a wide range of common technologies, it is not possible for NSA to provide specific guidance for every application of cryptography. In particular, cloud-based technologies and specific software toolkits may have their own names for various cryptographic selections or their own cryptographic protocols. Developers are expected to determine that the cryptography underlying their choices complies with CNSA 2.0, but NSA reserves the authority to determine the appropriateness of these choices if they are not built off certified products. NSA will respond to NSS users' specific questions as they arise.

Q: What is the difference between ML-KEM and CRYSTALS-Kyber, or between ML-DSA and CRYSTALS-Dilithium?

A: ML-KEM and ML-DSA are fully specified standards described by NIST in FIPS 203 and 204, respectively. CRYSTALS-Kyber is the name of the proposed algorithm submitted to NIST that eventually became ML-KEM, and similarly CRYSTALS-Dilithium became ML-DSA. In particular, the CRYSTALS algorithms had a variety of versions that included small tweaks made by the designers in cooperation with NIST prior to the publication of the FIPS documents. Once NIST announced the drafting of CRYSTALS-Kyber and CRYSTALS-Dilithium into standards, NSA announced that the standards



would be part of CNSA 2.0. NSA clarified the CNSA 2.0 language when the FIPS documents were published. Only ML-KEM and ML-DSA are in CNSA 2.0; any algorithm that is called CRYSTALS-Kyber or CRYSTALS-Dilithium but does not adhere to FIPS 203 or 204 is not CNSA 2.0 compliant.

Q: When should I use hash-based signatures, and which should I use?

A: NSA allows certain [NIST SP 800-208](#)⁷ standardized stateful hash-based signatures to secure firmware and software and their update processes. Due to the long-expected lifetime needed for many firmware, they urgently require implementing quantum-resistant algorithms.

In addition, firmware often must perform in constrained environments. Because many chips natively support hashing, this makes small hash-based signatures, such as LMS and XMSS, natural choices. NSA prefers the parameter set in Section 4.2, LMS with SHA-256/192, but any choice of XMSS or LMS satisfies CNSA 2.0 requirements.

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 multi-tree algorithms HSS and XMSSMT are not allowed.

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 for NSS. 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 and signers. If your product is only verifying signatures, CAVP testing is all that is required.

Code sources and signature generation processes (signers) that are NSS are required to produce signatures according to NIST SP 800-208, which requires hardware

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



validated by NIST's Cryptographic Module Validation Program (CMVP), or via other NSA guidance. Waivers for this will not be granted.

While code on devices used in an NSS must meet CNSA requirements, the signature generation processes for that code (signers) are often not themselves NSS. For example, for many commercial vendors with commodity products used in an NSS, their development environments are not NSS. In this case, those signers are expected to use code in their signature generation processes that is at least at the same operational quality as the code being put on the device, but the only part NSA will validate is that the signature verification code on the device passes CAVP.

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 started including quantum-resistant signatures consistent with NSA's published transition timelines. Where signing occurs outside the Target of Evaluation (TOE) boundary, such as for commercial products being certified where only firmware signature verification is performed within the TOE while the firmware signing is performed outside the TOE by an HSM or other external signing service, Protection Profile requirements only apply to 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 to meet CNSA 2.0 for such products.

Q: Why are signatures for software- and firmware-signing listed separately from signing other information?

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

- NIST standardized the algorithms in NIST SP 800-208 earlier and had CAVP validation available for many years, at a time when other quantum-resistant signatures were not as easily available for integration. Therefore, they are more broadly available in low-level hardware.



- This signature use case for firmware and software (especially firmware) is slightly more urgent at this time in the acquisition cycle as it must be QR at the time of acquisition (see the following question and answer for additional information).
- This selection places hash-based algorithms, with their substantial history of cryptanalysis, in a use case where their well-described potential performance issues—the requirement for keeping track of state and ensuring certain private data is not used more than once in signing software or firmware—have minimal impact.

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 its timelines to avoid unexpected costs and security issues later in the NSS transition.

Q: Under what circumstances is SHA-3 available for use?

A: At a vendor's discretion, for internal components of a hardware system that do not interoperate outside a vendor's environment, SHA3-384 or SHA3-512 may also be used as part of a system's integrity-checking process, such as secure boot. This is specifically being allowed in CNSA 2.0 to speed the transition process when vendor-specific internal processes make use of the properties of a cryptographic hash to enable them to transition to the new post-quantum signatures with minimal disruption to their workflow. In order not to be prescriptive in these cases, and due to the particular threat vectors inherent in these processes, NSA is allowing the use of either SHA-384, SHA-512, SHA3-384, or SHA3-512 for these purposes.

Q: Can I use SHA-3 in protocols that validate my virtual machines (VMs)?

A: Hardware is where one expects a hardware root of trust and where SHA-3 is allowed for use. At this time, VMs chaining back to a virtual root of trust should not use SHA-3 to cryptographically validate integrity.



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

A: No, neither SHA-3 nor SHAKE are approved for use in CNSA 2.0 as a general-purpose hash algorithm. While NSA allows any parameter set of LMS, including some that call SHA-3 as an internal function, NSA has not approved SHA-3 as a general-purpose 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, or for internal hardware system processes as described above.

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 completely self-contained, such as when called within an algorithm function, significantly increases the interoperability testing burden and breaks many use cases for CNSA 2.0.

Q: Can I use SHA-3 and SHA-256 for self-contained non-hash purposes, specifically as a pseudo-random function in deterministic random bit generators (DRBGs) and key derivation functions (KDFs), or as an alternative to XOR for combining submasks?

A: No. Unlike other algorithms in CNSA 2.0, no explicit carve outs say a specific DRBG is allowed, hence these higher-level primitives should be composed of CNSA 2.0 hashes or block ciphers. If there are specific places where SHA-3 or another hash is appropriate and approved, this will be clearly documented in NSA guidance, as was done with secure boot.

Q: Are there any plans to add SHA-3/SHAKE to the "General Purpose Algorithms" section of CNSA?

A: While there are no current plans to allow SHA-3/SHAKE on a wider scale, with SHA-3's current standing as a component in many primitives and its increasing adoption in networking standards, it would be prudent from a cryptographic agility perspective for NSS customers to have larger versions of SHA-3/SHAKE available in FIPS 140 validated products.



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

A: NIST's [post-quantum standardization page](#) includes reports from all the rounds of the standardization effort that detail why NIST chose lattice-based cryptography. These reports include summaries of all the cryptography that was 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. Since NIST has prioritized standardizing ML-DSA, FN-DSA is not available yet, and deployment of CNSA 2.0 needs to commence as soon as possible, NSA selected ML-DSA. NSA does not anticipate adding FN-DSA to CNSA 2.0 when it is available.

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

A: Yes, however, firmware roots of trust are a critical component to upgrade and NSA expects this to be implemented at the present time for some long-lived signatures. Given validated LMS and XMSS have been commercially available longer, NSA wants to ensure this transition can begin now (using LMS and XMSS) whenever possible, rather than wait for ML-DSA due to the long timeframes involved in moving from small components and/or early designs to completed products.

Validated ML-DSA is approved for all signing use cases, and it may be the most appropriate choice 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: Is HashML-DSA, also known as the pre-hash mode of ML-DSA, allowed in CNSA 2.0?

A: Not at the present time. HashML-DSA is a variant on ML-DSA in FIPS 204, which describes a method of compressing a message before signing while intentionally breaking interoperability with ML-DSA to prevent a vulnerability in the case of key re-use. HashML-DSA offers no additional functionality over existing CNSA hash functions combined in a standard way with ML-DSA-87, which is expected to be widely



supported. Therefore, NSA anticipates no need for HashML-DSA in NSS. For example, the [Commercial National Security Algorithm \(CNSA\) Suite 2.0 Profile for Certificates and Certificate Revocation Lists IETF draft](#) specifies how the external-μ functionality described in FIPS 204 can be used when signing a certificate with ML-DSA without having to invoke a separate hash function.

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, but adding more algorithms generally makes interoperability more complex.

Q: How is CNSA 2.0 implementation enforced in NSS?

A: Authorizing officials will be reporting regularly on adoption of CNSA 2.0 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. The authorizing officials must 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 cannot be used to protect NSS unless NSA has provided specific written guidance otherwise. CNSA 2.0 relies on NIST standardized algorithms that have been widely vetted as quantum resistant. Other algorithms should not be employed. Further, CNSSP 11 requires NIAP validation for commercial products used in NSS, and this validation will generally require CNSA 2.0 compliance.

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

A: When validated products become available, they should be deployed in mission systems. NIAP and the Commercial Solutions for Classified (CSfC) program both swiftly updated profiles as validation with new products became feasible. For systems outside these programs, refer to CNSSP 15 and future guidance for deprecation schedules of quantum-vulnerable cryptography.



Timeframe

Q: What is NSA's recommended timeframe for CNSA 2.0 adoption?

A: NSA intends that all NSS will be quantum-resistant well ahead of the 2035 goal outlined in NSM-10. The update to CNSSP 15 set several dates to aid in this transition in the commercial space, with the hope of completing much of the transition sooner.

CNSSP 15 states that by January 1, 2027, CNSA 2.0 algorithms will be required in all new acquisitions for NSS and NIAP Protection Profiles are being updated to enable QR certification before this date. Due to new rules limiting the life of NIAP validation certificates, all products certified before 2027 will require revalidation before the end of the decade.

By December 31, 2030, all NSS equipment and services that cannot support CNSA 2.0 must be phased out unless otherwise granted an exception. Because of how negotiation is performed in modern protocols, this is also the date at which NSA expects encryption to be broadly QR by default.

By December 31, 2031, CNSA 2.0 algorithms are mandated for use, unless otherwise noted, to achieve full QR for NSS.

Q: Will I need to transition all my algorithms at once to CNSA 2.0?

A: As NSS transition to CNSA 2.0 by 2031, NSA expects to have a long period of systems using both CNSA 1.0 and 2.0 in different places. New NSS developments will be required to support CNSA 2.0 algorithms 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 Standard Development Organizations (SDOs) develop the appropriate standards because product lines may develop at different speeds, and not every profile supporting CNSA 2.0 will support it for every cryptographic service offered. CNSA 1.0 algorithms will continue to be used until current solutions can operate in a CNSA 2.0 mode.



Q: What is the timeline for new deployments?

A: NIAP and the CSfC program will update their profiles and requirements in accordance with industry adoption. NSA intends an aggressive timeframe for adoption (see above) and requests industry support. Starting on January 1, 2027, NSA expects new deployments to be compliant with CNSA 2.0, unless otherwise explicitly noted in profiles.

Q: I am a vendor whose product was NIAP-certified before the QR requirements were finalized. What is my product's status?

A: NIAP will begin to archive partially QR and quantum-vulnerable product certificates generally within a year of fully QR products coming on the market. NSA expects this archiving to start in late 2027. At that point, products with archived certificates will not comply with CNSSP 11 and will not be appropriate for NSS.

Q: If no CNSA 2.0 compliant products meeting my needs are available on January 1, 2027, is it acceptable to purchase an updateable product and deploy the CNSA 2.0 options later?

A: NSA recognizes that in some product spaces, fully certified solutions may not be available for acquisition by the end of 2026. If needed, a deployment may be accepted based on a contractual commitment by a vendor to provide a CNSA 2.0 update when combined with a realistic deployment plan prioritizing partial QR that meets the 2030 deadline for full QR. However, this will need to be regularly tracked and reported to ensure final transition deadlines are met. Immediate implementation, followed by actual use of CNSA 2.0, should always be the preferred strategy. Moreover, some components, like firmware update options, likely cannot be transitioned after purchase, and customers are urged to make sure those services are QR at the time of purchase, or risk being required to purchase new products in 2030.

Q: What is the timeline for transitioning fielded equipment?

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

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.

NSA expects these equipment transitions to be completed by December 31, 2030, as mandated in CNSSP 15.

Q: When will IETF RFCs containing guidance on configurations for CNSA 2.0 compliant protocols be available?

A: These RFCs are being drafted now and will be finished soon.

The IETF and other SDOs are independent bodies in charge of their own publication schedules. Due to the interest in this guidance beyond standard NSA customers, and to facilitate quantum-resistant deployment more broadly, NSA is working with the IETF and other SDOs to produce RFCs and other documentation with the appropriate level of security and implementation analysis. NSA encourages CNSA 2.0 adoption in standards and deployment in vendor products, but it is not an NSA requirement beyond NSS.

CNSSP 15 and NSM-10

Q: What is National Security Memorandum (NSM) 10?

A: National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems lays out tasks for the federal government with the goal of achieving quantum resistance by 2035, including the creation of quantum-resistant standards and the deprecation of quantum-vulnerable standards. NSA is explicitly called out to provide timely guidance for quantum resistance in NSS, and NSS owners are given annual reporting requirements for quantum-vulnerable systems.

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” as the required commercial algorithms for protecting NSS, and then it was revised to specify



the CNSA 1.0 Suite in CNSSP 15 Annex B. It now includes CNSA 2.0 algorithms since NIST has completed its initial standards from its Post-Quantum Standardization Process. CNSSP 15 also includes a mandated timeline for adoption of CNSA 2.0 algorithms in NSS. Further details about CNSS are at www.cnss.gov.

Q: What changes are in the CNSSP 15 update?

A: Based on NSM-10, the 2024 update to CNSSP 15 makes three significant changes:

1. It updated the list of allowed algorithm standards, which was previously defined as CNSA 1.0, to now require CNSA 2.0. This deprecated all quantum-vulnerable algorithms, added quantum-resistant public key mechanisms, as well as added SHA-512 into general usage and SHA-3 into specific applications.
2. It set out dates for the transition from CNSA 1.0 to CNSA 2.0, including adoption dates for new systems, as well as deprecation dates for currently deployed systems.
3. It revoked the previous eight years of waivers to CNSSP 15, which therefore requires modernization of several NSS.

Q: As an NSS owner, when will my quantum-resistant transition be completed according to the reporting requirements under NSM-10?

A: As noted in CNSSP 15, if any component of an NSS is not quantum-resistant, reporting requirements continue under NSM-10. While CNSSP 15 allows the use of currently validated profiles that rely on CNSA 1.0, if a profile requires any non-CNSA 2.0 algorithm to function securely (such as those in CNSA 1.0), it will be reportable under NSM-10. NSA expects this to continue for many customers through December 31, 2031, when cryptography in NSS should be quantum resistant.



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

A: [CNSS Instruction 1253](#)⁸ mandates using the Risk Management Framework (RMF) as documented in [NIST SP 800-39](#)⁹ and [NIST SP 800-53](#)¹⁰ 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 2.0 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 protection requirements. Often these systems require protection for long periods against sophisticated targeted efforts and well-resourced adversaries in potential wartime settings. NIST establishes cryptographic standards for other government systems.

NSA selected the algorithms in CNSSP 15 from those chosen by NIST to satisfy NSA requirements for NSS and 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](#).¹¹

Q: Are there other broad government policies to transition to QR algorithms?

A: Executive Order 14412 sets a timeline for high value assets and high impact systems in the Federal/Civilian Executive Branch (FCEB) to use QR algorithms by 2031 at the latest.

⁸ Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems.

⁹ NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

¹⁰ NIST Special Publication 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations.

¹¹ NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.



In addition, NIST stated in NISTIR 8647 that it will disallow quantum-vulnerable algorithms in NIST validation processes in 2035, meaning that those algorithms will likely stop being available in the marketplace as the transition continues.

Q: How does the recent Executive Order 14412 impact your guidance?

A: NSA expects NSS to satisfy the timelines within EO 14412 by following the requirements in CNSSP 15.

Transition timelines within EO 14412 apply to non-NSS systems in the FCEB and do not change CNSS Policy 15 and its timeline for NSS transition to CNSA 2.0. NSS and commercial products used in NSS will transition according to the schedule established in CNSS Policies, which is at least as fast as the EO.

The EO requires that directed FCEB systems use post-quantum confidentiality (i.e., key establishment) by the end of 2030 and full QR (i.e., including digital signatures for authentication) by the end of 2031. While these timeline requirements do not apply to NSS, NSS has comparable requirements and timelines in CNSSP 15. The CNSSP 15 2030 deadline requires that NSS equipment support CNSA 2.0 and be QR capable. CNSA 2.0 capability, combined with modern protocols that negotiate the most secure encryption, means that NSS are required to have QR encryption in place no later than when the EO requires for FCEB. Systems that use products validated against CNSA 2.0 compliant Protection Profiles can meet these deadlines.

Quantum alternatives

Q: Can I mitigate the quantum threat to NSS 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 and using pre-shared keys or a combination of keys may be prohibited by policy for some customers. Customers who wish to explore this option for their long-lived or low-powered systems 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: NSM-10 documents specific requirements for NSA to provide quantum resistance for NSS by 2035, requiring significant steps over the next several years. Further, government procurement timelines drive NSA to strongly encourage and support commercial QR technology availability by 2027.

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. Research on quantum computing is progressing, so NSA must act now to protect NSS by providing these CNSA 2.0 transition requirements and guidance today.

Q: I just read a news report or scientific paper asserting quantum computers are coming soon. Is NSA's timeline correct?

A: As with any emerging technology, breakthroughs, claims, and new barriers to progress are to be expected and will continue to appear. This is an evolving area with many opinions. NSA monitors work in this area and believes the currently established timelines are the most responsible choice given where customers are today with the long-term mitigations. NSA will notify the NSS community if changes to timelines are required, but NSA does not anticipate any changes at this time. Other communities may have different circumstances and may follow different timelines.



Q: Given the threat, is the NSS community moving aggressively enough to mitigate the impact of an early CRQC?

A: NSA has been at the forefront of mitigating the quantum threat to cryptography for years. NSA believes that the currently established timelines are appropriate to address the expected threat. Since 2016, small elliptic curves have been deprecated in NSS. With the signing of CNSSP 15 in 2025, exemptions to this were revoked. Currently, compliant devices should be using either Curve P-384, RSA with at least a 3072-bit modulus, or an NSA-approved alternative. A sufficiently capable CRQC would be necessary to undermine these algorithms and key sizes. Further, the transition to QR algorithms is already underway and proceeding with urgency. Starting in 2027, no new product for NSS should have a burned-in root of trust relying on a non-QR primitive. By the end of 2030, all available devices should fully support QR algorithms.

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?

A: A quantum random number generator (RNG), also called a Quantum RNG or a QRNG, is a hardware RNG that uses specific quantum effects to generate nondeterministic randomness. CNSS policy does not favor quantum RNGs versus other



types of RNGs, and 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 when implemented within the constraints of that approval. As a reminder, regardless of quantum or traditional, all commercial RNGs used in NSS must generally at least satisfy [NIST SP 800-90 A](#), [B](#), and [C](#).

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

Q: Can I use any CNSA-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. In situations where NIAP and FIPS validation are not possible, CNSSP 11 requires consulting NSA for a risk determination. This should only be used in limited circumstances. NIAP and FIPS validation are required in most circumstances.

Furthermore, CNSSP 7 states that a CSfC solution may protect classified NSS information at a lower level of classification, provided the appropriate Authorizing Official approved it and registration with NSA's CSfC Program Management Office showed it is 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: CSfC has updated all existing Capability Packages with guidance on quantum resistance. As NIAP continues to certify QR components, the number of CSfC solutions that are inherently QR will grow. Further, some CSfC solutions may be implemented today using symmetric, pre-shared keys that protect against the long-term quantum computing threat. Users seeking an accelerated transition should [contact NSA](#) on whether packages leveraging pre-shared symmetric keys in a standards-compliant fashion are a reasonable near-term QR solution. 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 innovations). 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 on NSS.

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 manages efforts, such as NIAP and the CSfC program, that require strict compliance 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.

Q: Will NSA be adopting the standards from NIST's Post-Quantum Signature On-Ramp effort?

A: NSA currently does not expect to integrate the results of the On-Ramp effort into future CNSA versions. ML-DSA is effective for a broad range of NSS and is presently available.

Q: What does this mean for cryptocurrencies?

A: Cryptocurrencies are typically not considered NSS, primarily because they are not operated or managed by the U.S. Government. Thus, they are not an NSA responsibility. In general, communities that support or operate cryptocurrencies are making their own risk determinations, timelines, algorithm selections, and transition plans, and they may choose whether to follow NSA public guidance.

Hybrids and composites

Q: What is a hybrid or composite cryptographic solution?

A: NSA views a hybrid solution for a protocol as one that uses multiple algorithms to perform the same function, such as key agreement or authentication. The solution uses algorithms in a way that requires an adversarial actor 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. In some



circumstances, such as in forums discussing public key certificates, the word "composite" is used instead. This document uses the two terms interchangeably.

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. However, product availability and interoperability requirements may lead to adopting hybrid solutions in specific cases.

NSA recognizes that some protocols may require using hybrid-like constructions to accommodate the larger sizes of ML-KEM-1024 or ML-DSA-87 and will work with industry and SDOs to identify the best options for implementation. In these cases, where NSA worked with SDO and provided public guidance on hybrid use, only the hybrid solution identified by NSA would be considered "CNSA 2.0 compliant."

Q: If I use a hybrid solution in my NSS, am I quantum resistant?

A: NSS is only considered compliant and quantum resistant when using CNSA 2.0 algorithms in an NSA-approved manner, such as when validated against an appropriate NIAP Protection Profile. While hybrid standards that use NIST standards exist in many SDOs, very few use CNSA 2.0 algorithms. Moreover, design choices of whether to negotiate a hybrid, what format to have in a certificate, etc. are often unclear. As a result, something marketed as hybrid or composite does not necessarily make it quantum resistant.

Q: What complications do hybrid solutions introduce?

A: Hybrid solutions add complexity to protocols and cryptographic libraries, as designers need to incorporate additional negotiation and error handling and implementers need to modify APIs and testing.

Rather than ease the transition to quantum resistance, hybrid deployments can introduce additional interoperability concerns because all the algorithms and the method of hybridization must be features common to all parties in communication. Similarly, hybrid deployments add a second transition later as users eventually move away from classical algorithms entirely in the future and use only quantum-resistant algorithms.

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 weaken security rather than improve it. Indeed, for some formal security properties, hybrids may be no stronger, or possibly even weaker, than their individual components. This is a matter of significant debate in industry and academia.

In many scenarios, adding a hybrid option will require the standards community to determine non-obvious choices, such as how to negotiate hybrid algorithms or how to combine keys securely, which may slow down the process of standardization past NSA's deployment goals.

When NSA recognizes a need to support a hybrid solution, extensive work is performed to ensure that it can be expected to be implemented properly, including engineering the solution to a high degree of robustness.

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

A: Due to difficulties introduced when unencrypted IKEv2 messages exceed a certain byte size, it is not possible to directly replace the CNSA 1.0 public key algorithms with ML-KEM-1024 and its larger public key. Because there is no straightforward way to construct a solution that uses a standalone ML-KEM-1024 key establishment without dramatic changes to this part of IKEv2, NSA approved using the solution standardized within the IETF. This solution effectively manages this problem by performing a smaller key establishment, followed by a larger, but encrypted, key establishment. As a result, for the foreseeable future, NSA's CNSA 2.0 Profile of this solution will continue using CNSA 1.0 key establishment algorithms but fortified by key establishment using ML-KEM-1024 from CNSA 2.0.

Q: I don't want to tear out my quantum-vulnerable root of trust today. Do I need to use a composite signature?

A: No. PKI systems have historically undergone several algorithm transitions, to include changing hash functions and migrating from RSA to ECC. Importantly, in all these historical transitions, owners were able to continue using their old certificates as they migrated to newer signatures. In each case, the approach chosen involved standing up a parallel PKI using the new cryptographic algorithm rather than attempting to add an



additional algorithm into an existing PKI structure. PKI transitions will use existing formats, simply replacing the algorithms with the new CNSA 2.0 options, and transitioning as new credentials are issued. This will mean that, in some cases, devices expected to be removed from the network may have only quantum-vulnerable identity credentials; new devices may have only quantum-resistant identity credentials; and other devices may have two identity credentials (one from each chain) for interoperability until the transition completes.

The reasons for the parallel PKI approach have not changed from other historical transitions for the transition to QR algorithms. NSS, and the broader community, can benefit from lessons learned with this being a well-trod path. NSS systems using PKI should not use novel mechanisms to support multiple algorithms within a single certificate.

Q: Should one use a hybrid or other non-standardized QR solution while waiting for a final post-quantum protocol standard for any specific technologies?

A: Do not use any non-standardized QR solution on NSS mission systems except for those exceptions NSA specifically recommends to meet standardization or interoperability requirements. Because NSA is confident that CNSA 2.0 algorithms will sufficiently protect NSS, it does not require a hybrid solution for security purposes. Importantly, it is unlikely a non-standardized solution used in testing will be able to be integrated into eventual deployable solutions.

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 8773](#), [RFC 8784](#)) may be appropriate, but key management complexity generally restricts this to specialized applications.

Additional 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 through normal business channels.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, 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 War, 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