THE CURRENT STATE OF ENCRYPTION CAPABILITIES

FROM CLASSICAL CRYPTOGRAPHY TO THE QUANTUM-RESISTANT FUTURE

White Paper

5285 Shawnee Road, Suite 400
Alexandria, Virginia 22312
(703) 564-3800
www.mtsi-va.com

Technical Point of Contact
Marc Kolenko, ScD, MTSI Telecommunications Technical Fellow
for Command, Control & Communications
(703) 638-5977
marc.kolenko@mtsi-va.com

Written: June 2026

RESTRICTED DATA NOTICE

This white paper includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to inform the National Geospatial-Intelligence Agency (NGA) data storage, compute, and networks modeling, simulation, and analysis. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. This restriction applies to the entire white paper.

AI Usage Disclosure (Optional)

This document was created with assistance from AI tools and has been reviewed and edited by a human. Please note that AI-generated content may contain errors or inaccuracies. Users should exercise caution and conduct their own verification before relying on this information.

CONTENTS

1 EXECUTIVE SUMMARY

Encryption is the bedrock of data protection across both the private and public sectors. As cyber threats grow in sophistication and scale, the algorithms that safeguard financial transactions, classified intelligence, health records, and critical infrastructure are under unprecedented scrutiny. For defense contractors, government agencies, and the technology providers that support them, understanding the current encryption landscape is not merely a technical exercise — it is a strategic imperative.

Today, organizations rely on a multi-layered cryptographic approach that combines symmetric encryption (principally AES) for high-speed bulk data protection, asymmetric encryption (RSA, ECC) for secure key exchange and digital signatures, and hybrid models that unite the strengths of both. These mechanisms protect data at rest and in transit across every layer of the modern technology stack, from TLS-secured web traffic to encrypted storage volumes and signed firmware images.

However, the emergence of quantum computing introduces a paradigm-level threat to this foundation. A sufficiently powerful quantum computer running Shor's Algorithm could break the mathematical problems underpinning RSA and ECC in a fraction of the time required by classical machines — rendering current asymmetric encryption obsolete. Symmetric algorithms such as AES-256 are more resilient; Grover's Algorithm provides only a quadratic speedup to brute-force key search, reducing effective security from 2256 to 2128 — a level that remains computationally infeasible.

The U.S. government has responded decisively. The NSA's CNSA 2.0 roadmap mandates a phased transition to quantum-resistant algorithms — including ML-KEM (CRYSTALS-Kyber) for key establishment, ML-DSA (CRYSTALS-Dilithium) for digital signatures, and LMS/XMSS for software and firmware signing — with full migration across all National Security Systems targeted by 2035.

The timeline for action has compressed dramatically. In March 2026, Google — which simultaneously operates one of the world's most advanced quantum computing programs and maintains critical global internet infrastructure — announced a hard target of 2029 to complete its post-quantum cryptography migration, a full year ahead of NIST's planned deprecation and six years ahead of the final disallowance deadline. This signal from a company uniquely positioned at the intersection of quantum hardware development and global-scale infrastructure defense underscores that the transition window is shorter than most organizations have planned for.

This white paper provides a comprehensive analysis of the modern encryption landscape, the nature and timeline of the quantum threat, the government's evolving cryptographic standards, and actionable guidance for organizations preparing for the post-quantum era.

Beyond the immediate CNSA 2.0 migration imperative, a second emerging capability warrants strategic attention: Homomorphic Encryption (HE). While post-quantum algorithms address the security of data in transit and at rest, HE closes a third and final gap — protecting data while it is actively being processed. By enabling mathematical operations to be performed directly on ciphertext, HE eliminates the requirement to decrypt data before computation, removing the plaintext exposure window that exists in every conventional processing architecture. Though still maturing — with current Technology Readiness Levels of 4–6 — HE is advancing rapidly under DARPA DPRIVE and IARPA investment programs, and NSA has identified it as a priority privacy-enhancing technology. Organizations building long-term cryptographic architectures should begin tracking HE scheme development and piloting use cases now.

▸ **KEY TAKEAWAY**: *The transition to quantum-resistant cryptography is not a future concern — it is an active mandate. Organizations must begin cryptographic inventory and migration planning now to meet CNSA 2.0 deadlines, with software/firmware signing transitions required by 2030 and networking equipment support required by 2026. Additionally, Homomorphic Encryption emerges as a strategic complement to CNSA 2.0 — enabling computation on ciphertext and extending zero-trust data protection to active processing environments.*

2 FOUNDATIONS OF MODERN ENCRYPTION

In both the private and public sectors, the security of information is paramount. Encryption stands as a primary defense, converting sensitive data into an unreadable format to shield it from unauthorized access. Financial institutions and government agencies employ a variety of encryption algorithms to protect data both when it is being stored (at rest) and when it is being transmitted (in transit). The sections that follow provide a detailed examination of the principal cryptographic methods in use today, the protocols that apply them, and the security properties they provide.

2.1 Symmetric Encryption

Symmetric encryption utilizes a single key for both the encryption and decryption of data. This method is known for its speed and efficiency, making it well-suited for encrypting large volumes of data. Because the same key must be shared between the encrypting and decrypting parties, secure key distribution is a critical concern — one that is typically addressed through asymmetric or hybrid methods described later in this paper.

Table 1: Symmetric Encryption Algorithms

Algorithm	Key Details	Common Uses in Finance/Government
Advanced Encryption Standard (AES)	The current industry standard, offering key sizes of 128, 192, and 256 bits. Recognized for high security and efficiency.	Securing sensitive data, protecting customer data, and securing data at rest and in transit.
Triple Data Encryption Standard (3DES)	An older algorithm that applies the DES cipher three times to each data block. It is being phased out in favor of AES.	Used in some legacy banking systems and for securing credit card transactions.
Data Encryption Standard (DES)	One of the first widely used algorithms. Its 56-bit key is now considered insecure against modern computing power.	Largely replaced by more secure algorithms like AES and 3DES.

Blowfish and Twofish	Blowfish is a fast symmetric-key block cipher. Twofish is its successor with a 128-bit block size and keys up to 256 bits.	Used in database security, e-commerce platforms, and file encryption.

2.2 Asymmetric Encryption

Also known as public-key cryptography, asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. This method is fundamental for secure communication over public networks, as it eliminates the need for both parties to possess a pre-shared secret. Asymmetric algorithms also enable digital signatures, which verify the authenticity and integrity of data.

Table 2: Asymmetric Encryption Algorithms

Algorithm	Key Details	Common Uses
RSA (Rivest-Shamir-Adleman)	A widely used algorithm whose security is based on the difficulty of factoring large prime numbers.	Digital signatures, secure data communications, and securing the exchange of symmetric keys.
Elliptic Curve Cryptography (ECC)	Offers security comparable to RSA but with smaller key sizes, making it efficient for mobile and IoT devices.	Digital signatures, key exchange, and securing communications in resource-constrained environments.
Diffie-Hellman Key Exchange	A method for two parties to securely establish a shared secret key over an insecure channel.	Used to secure a wide range of internet services.
Algorithm	Key Details	Common Uses

2.3 Hybrid Encryption

To leverage the strengths of both symmetric and asymmetric encryption, institutions often employ a hybrid approach. This method uses asymmetric encryption to securely exchange a symmetric key, which is then used for the faster encryption of the bulk of the data. The asymmetric layer solves the key-distribution problem, while the symmetric layer provides the throughput needed for large data volumes.

This hybrid model is the dominant paradigm in virtually all real-world secure communications. The TLS handshake — the protocol that secures every HTTPS connection on the internet — is a canonical example. During a TLS session, the client and server use asymmetric cryptography (such as RSA or ECDH) to negotiate a shared session key, which is then used with a symmetric cipher (typically AES) to encrypt the actual data payload. This same pattern is replicated in VPN tunnels, encrypted email (S/MIME, PGP), secure file transfer protocols, and virtually every other modern encryption deployment. The hybrid model balances the security of asymmetric key exchange with the performance of symmetric bulk encryption, and it is the reason that both classes of algorithm are critical to the overall security posture of any organization.

2.4 Securing Data in Transit

For data moving across networks — such as during online banking, mobile payments, inter-agency communications, or cloud service interactions — protocols like Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are used. These protocols use encryption to create a secure channel between a client and a server, protecting against eavesdropping and tampering. TLS negotiates the cipher suite, performs the key exchange, and then encrypts the session data, ensuring that even if an attacker intercepts the traffic, the content remains unreadable.

2.5 Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy is a security feature ensuring that a compromised long-term server key cannot be used to decrypt past recorded conversations. It works by generating a unique, temporary (ephemeral) key for each session, which is discarded after the session ends. This prevents a single point of failure and dramatically limits the impact of a key theft. PFS is commonly enabled by protocols like ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), which generates a fresh key pair for every handshake, ensuring that the compromise of any one session key reveals nothing about past or future sessions.

▸ **WHY PFS MATTERS**: *Without Perfect Forward Secrecy, an attacker who compromises a server's private key can retroactively decrypt all previously recorded sessions. PFS ensures that even a catastrophic key compromise is limited to the single session in which it occurs. In an era where adversaries may employ "harvest now, decrypt later" strategies — recording encrypted traffic today with the intent of breaking it when quantum computers mature — PFS provides a critical additional layer of defense.*

3 Government Cryptographic Standards: From Suite B to CNSA 2.0

The U.S. government has maintained a structured, evolving approach to cryptographic standardization for National Security Systems (NSS). Over the past two decades, the National Security Agency (NSA) has published and updated its recommended algorithm suites in direct response to advancing computational threats — progressing from the classical foundation of Suite B through the transitional CNSA 1.0, and now to the quantum-resistant mandate of CNSA 2.0. Understanding this evolution is essential for any organization operating within or supporting the defense communities.

3.1 NSA Suite B (2005): The Classical Foundation

NSA Suite B was a set of cryptographic algorithms selected by the U.S. National Security Agency (NSA) in 2005 to protect government information. It established a standardized, interoperable cryptographic foundation for securing classified and sensitive communications across the federal enterprise.

The primary purpose of Suite B was to provide a uniform set of strong, publicly available cryptographic algorithms that could be implemented in commercial products to protect U.S. National Security Systems. This allowed for secure communication and data protection across various government agencies and systems. The standard was conceptually similar to FIPS 140-2, as it restricted the set of enabled cryptographic algorithms to ensure a certain level of security, while encouraging broad commercial adoption and interoperability.

Table 3: Core Components of NSA Suite B

Cryptographic Function	Algorithm	Details
Encryption	Advanced Encryption Standard (AES)	128-bit keys for SECRET, 256-bit keys for TOP SECRET
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA)	Utilized the P-256 and P-384 curves
Key Exchange	Elliptic Curve Diffie-Hellman (ECDH)	Employed the P-256 and P-384 curves
Hashing	Secure Hash Algorithm 2 (SHA-2)	Specifically, SHA-256 and SHA-384

3.2 The Transition: From Suite B to CNSA

In 2015, the NSA replaced Suite B with the Commercial National Security Algorithm (CNSA) Suite. This transition was driven by advancements in computing and the future threat of quantum computers, which could potentially break many of the algorithms used in Suite B. The CNSA 1.0 suite retained many of the same algorithm families (AES, SHA, RSA, ECDSA, ECDH) but specified stronger parameters — larger key sizes and more robust curves — to extend the security runway while the cryptographic community developed truly quantum-resistant replacements.

3.3 CNSA 2.0: The Quantum-Resistant Era

The Commercial National Security Algorithm (CNSA) Suite is the NSA's current set of cryptographic algorithms. CNSA 2.0, announced in 2022, guides the transition to quantum-resistant cryptography to counter the threat of a cryptanalytically relevant quantum computer (CRQC). To counter this, the U.S. government has mandated a transition to quantum-resistant (QR) algorithms, with the goal of mitigating most of the quantum risk by 2035. CNSA 2.0 is the NSA's roadmap for achieving this security for National Security Systems.

CNSA 2.0 specifies a set of algorithms for different cryptographic functions, mandating quantum-resistant solutions for public-key cryptography while retaining robust symmetric algorithms that are already considered quantum-safe at sufficient key lengths.

Table 4: Key Changes from CNSA 1.0 to CNSA 2.0

Use Case	CNSA 1.0 (Pre-Quantum)	CNSA 2.0 (Quantum-Resistant)
Key Establishment	ECDH P-384, RSA-3072, DH-3072	ML-KEM-1024
Digital Signature	ECDSA P-384, RSA-3072	ML-DSA-87
Software/Firmware Signing	ECDSA P-384, RSA-3072	LMS or XMSS (Hash-Based Signatures)
Symmetric Encryption	AES-256	AES-256 (Unchanged)

Table 5: Core Components of CNSA 2.0

Function	Algorithm	Specification
Symmetric Encryption	Advanced Encryption Standard (AES)	FIPS PUB 197
Public Key Establishment	ML-KEM (CRYSTALS-Kyber)	FIPS PUB 203
Digital Signature	ML-DSA (CRYSTALS-Dilithium)	FIPS PUB 204
Hashing	Secure Hash Algorithm (SHA)	FIPS PUB 180-4

4 The Quantum Computing Threat

Quantum computing represents a paradigm shift not only for computation in general but for the field of cryptography in particular. While classical computers process information as binary bits (0 or 1), quantum computers exploit the principles of superposition and entanglement to process information in fundamentally different ways. For most computational tasks, this difference is academic. For cryptography, it is existential — because certain quantum algorithms can solve, in feasible time, the exact mathematical problems upon which modern public-key cryptography depends.

4.1 Asymmetric vs. Symmetric Vulnerability

Quantum computers pose a different level of threat to different types of encryption. The distinction is critical for prioritizing migration efforts:

- **Asymmetric Cryptography** (RSA, ECC): *Highly vulnerable.* Shor's Algorithm, a quantum algorithm, can solve the underlying math problems (e.g., integer factoring, discrete logarithms) exponentially faster than any known classical algorithm, effectively breaking this type of encryption entirely.
- **Symmetric Cryptography** (AES-256): *Resistant*. Grover's Algorithm can speed up a brute-force search for a symmetric key, but only quadratically. For AES-256, this reduces the effective security from 2256 to 2128, which is still considered computationally infeasible to break with any foreseeable technology.

4.2 Shor's Algorithm: The Existential Threat to Public-Key Cryptography

Classical asymmetric cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC) rely on mathematical problems that are computationally hard for traditional computers to solve, such as factoring large numbers or computing discrete logarithms. However, quantum computers, with algorithms like Shor's Algorithm, can solve these specific problems exponentially faster. This means that a sufficiently powerful quantum computer could break current RSA and ECC encryption relatively easily, rendering decades of cryptographic infrastructure obsolete.

Shor's Algorithm is not a general-purpose factoring tool. It is a period-finding algorithm. It works because the problem of factoring can be cleverly transformed into finding the period of a specific mathematical function (ax mod N). This function has a repeating, predictable structure that the Quantum Fourier Transform can efficiently detect. The algorithm exploits the inherent mathematical structure of the problem — structure that classical computers cannot leverage, but that quantum superposition reveals.

ANALOGY: *Shor's Algorithm is like trying to find the frequency of a sound wave in a recording. The wave has a clear, repeating structure (a period), and a tool like a Fourier transform is specifically designed to find that frequency. The quantum computer doesn't search for the answer — it resonates with the structure of the problem and reads the answer directly.*

4.3 Grover's Algorithm: Symmetric Cryptography's Resilience

Symmetric-key algorithms like AES work differently. They don't rely on these specific mathematical problems. Instead, their security is based on the difficulty of finding the correct key by brute-force search. A quantum algorithm called Grover's Algorithm can theoretically speed up brute-force searches. However, its speed-up is only quadratic, not exponential — a crucial distinction.

Grover's Algorithm is designed for the exact opposite scenario: a brute-force search where you have no helpful structure. You have a massive list of items and a way to check if an item is the one you're looking for, but you have no clues about where the correct item might be. There is no pattern to exploit, no periodicity to detect — only an exhaustive search, conducted more efficiently through quantum amplitude amplification.

▸ **ANALOGY:** *Grover's Algorithm is like trying to find a specific person's name in a phone book that has been completely scrambled. You have no alphabetical order to help you. Your only option is to start checking names one by one until you find the right one. Grover's just lets you check the names in a much faster, quantum way — but it still must check them. There is no shortcut to exploit, only speed.*

4.4 Comparative Analysis: Shor's vs. Grover's Algorithm

The following table summarizes the fundamental differences between the two quantum algorithms most relevant to cryptography, and why they produce such different impacts on asymmetric and symmetric encryption respectively:

Table 6: Shor's Algorithm vs. Grover's Algorithm

Feature	Shor's Algorithm	Grover's Algorithm
Primary Purpose	To find the prime factors of a large integer	To find a specific item in an unsorted database

Degree of Speed-up	Exponential	Quadratic
Cryptographic Target	Asymmetric Cryptography (RSA, ECC)	Symmetric Cryptography (AES)
Impact on Security	Breaks them completely	Weakens them, requiring longer keys for equivalent security

4.5 4.5 Google's 2029 Warning: The Timeline Accelerates

On March 25, 2026, Google published a consequential blog post authored by Heather Adkins, Vice President of Security Engineering, and Sophie Schmieg, Senior Staff Cryptography Engineer, titled "Quantum frontiers may be closer than they appear." In it, Google announced a hard target of 2029 to complete its migration to post-quantum cryptography — a full year ahead of NIST's planned 2030 deprecation date and six years ahead of the 2035 final disallowance deadline.

This announcement carries extraordinary weight because of Google's unique dual position: the company simultaneously operates one of the world's most advanced quantum computing research programs and maintains the infrastructure behind the world's most widely used browser, one of two dominant mobile operating systems, and a major cloud platform. When the company building the quantum computer tells the industry the clock is running out, the signal demands attention.

Two milestones underpin the urgency:

- **The Willow Chip** (December 2024): Google's Willow quantum processor demonstrated below-threshold quantum error correction for the first time — a foundational milestone that moves the field measurably closer to fault-tolerant, cryptanalytically relevant quantum machines.
- **The Gidney Research** (May 2025): Google researcher Craig Gidney and colleagues published findings showing that a 2,048-bit RSA key could be broken in under one week by a quantum computer with approximately one million noisy qubits. This represents a 20-fold reduction from the team's 2019 estimate, which projected roughly 20 million qubits would be required. The pace of this improvement — collapsing the resource estimate by an order of magnitude in just six years — illustrates how rapidly the threat horizon is compressing.

Google has already begun acting on its own warning. Android 17 will integrate ML-DSA (the NIST-standardized post-quantum digital signature algorithm) into the hardware root of trust, the Android Keystore, and the Play Store's developer signature infrastructure. This represents the first large-scale consumer platform migration to post-quantum cryptography.

▸ **INDUSTRY INFLECTION POINT:** *Google's 2029 migration deadline is not a theoretical planning exercise — it is a commitment by the company with the deepest insight into both quantum hardware progress and global internet infrastructure. Organizations that continue to*

benchmark their migration timelines against NIST's 2035 outer bound may find themselves critically exposed years before that deadline arrives.

5 The Post-Quantum Cryptographic Toolkit

In response to the quantum threat outlined in the previous section, the cryptographic community — led by NIST and the NSA — has developed and standardized a new generation of algorithms designed to resist attacks from both classical and quantum computers. These algorithms form the core of the CNSA 2.0 mandate and represent the building blocks of the post-quantum security architecture.

5.1 ML-KEM (CRYSTALS-Kyber): Quantum-Resistant Key Exchange

ML-KEM (Module-Lattice-based Key Encapsulation Mechanism), widely known by its original name CRYSTALS-Kyber, is a quantum-resistant algorithm designed for secure key exchange. Its primary purpose is to allow two parties to establish a shared secret key over an insecure channel, even in the presence of an adversary with a powerful quantum computer.

In July 2022, after a multi-year competition evaluating dozens of candidate algorithms, the U.S. National Institute of Standards and Technology (NIST) selected CRYSTALS-Kyber as the new standardized algorithm for public-key encryption and key establishment. It was formalized in the FIPS 203 publication under the name ML-KEM. The algorithm's security is based on the hardness of the Module Learning With Errors (MLWE) problem — a mathematical problem from lattice-based cryptography that is believed to be resistant to both classical and quantum attacks.

ML-KEM is a key component of the NSA's Commercial National Security Algorithm (CNSA) 2.0 suite, designated as the successor to classical key exchange methods like Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). CNSA 2.0 mandates the use of ML-KEM-1024, which provides NIST Security Level V — the highest assurance level.

5.2 ML-DSA (CRYSTALS-Dilithium): Quantum-Resistant Digital Signatures

ML-DSA (Module-Lattice-based Digital Signature Algorithm), originally known as CRYSTALS-Dilithium, is the standardized quantum-resistant algorithm for creating digital signatures. Its primary role is to verify the authenticity and integrity of data — ensuring that a message, document, or software package was created by a known sender and has not been tampered with.

Digital signatures are used to prove that a message or piece of data was sent by a specific party and that it has not been altered since it was signed. This is crucial for things like software updates, legal documents, and secure communications. ML-DSA is formalized in FIPS 204 and, like ML-KEM, derives its security from lattice-based mathematical problems. CNSA 2.0 mandates the use of ML-DSA-87 (Security Level V) for digital signature operations across National Security Systems.

5.3 SHA-384/SHA-512: Proven Hashing in the Quantum Era

SHA (Secure Hash Algorithm) is a family of cryptographic functions used to create a unique, fixed-size fingerprint of digital data, known as a hash. Unlike the other algorithms in CNSA 2.0, the recommended SHA algorithms are not new and have been the standard for years because they are not believed to be vulnerable to quantum attacks. Hash functions do not rely on the mathematical structures (factoring, discrete logarithms) that Shor's Algorithm exploits.

CNSA 2.0 mandates the use of either SHA-384 or SHA-512. These algorithms produce a 384-bit or 512-bit hash, respectively, providing a very high level of collision resistance (meaning it is practically impossible for two different inputs to produce the same hash). Their continued inclusion in CNSA 2.0 reflects the fact that well-parameterized symmetric and hash-based constructions remain secure in the quantum era.

5.4 LMS and XMSS: Hash-Based Signatures for Software Integrity

LMS (Leighton-Micali Signature) and XMSS (eXtended Merkle Signature Scheme) are stateful hash-based signature schemes. They are mandated for a very specific, high-assurance use case: signing software and firmware. Their security derives entirely from the properties of cryptographic hash functions, making them among the most conservative and well-understood quantum-resistant constructions available.

LMS and XMSS are standardized in NIST SP 800-208. The "stateful" nature of these schemes means that the signer must carefully track which one-time keys have been used — reusing a key compromises security. This operational constraint makes them best suited for controlled environments like firmware signing infrastructure, rather than general-purpose digital signatures. The NSA has prioritized their adoption for software/firmware signing, with a deadline for exclusive use by 2030.

5.5 CNSA 2.0 Transition Timeline

The NSA has laid out an aggressive but phased timeline for adoption, with a goal to have all National Security Systems quantum-resistant by 2035. The phased approach reflects the varying complexity and risk profile of different system categories:

Table 7: CNSA 2.0 Migration Milestones

System Category	Must Support CNSA 2.0 By	Exclusive Use Required By
Software and Firmware Signing	Transitioning immediately	2030
Web Browsers and Cloud Services	2025	2033
Traditional Networking Equipment (e.g., VPNs)	2026	2030
Operating Systems	2027	2033

▸ **CRITICAL DEADLINE:** *Web browsers and cloud services were required to begin supporting CNSA 2.0 algorithms by 2025. Traditional networking equipment must follow by 2026. Organizations that have not yet begun their cryptographic transition are already behind*

the NSA's recommended schedule. Delays compound risk: every month without migration extends the window during which adversaries can harvest encrypted data for future quantum decryption.

6 HOMOMORPHIC ENCRYPTION: COMPUTING ON CIPHERTEXT

▸ **STRATEGIC FRAMING**: *HE and PQC are complementary, not competing, security capabilities. CNSA 2.0 post-quantum algorithms secure the channel — protecting data in transit and at rest from quantum-capable adversaries. Homomorphic Encryption secures the computation — protecting data from exposure during processing, regardless of the threat actor. A complete zero-trust cryptographic architecture ultimately requires both.*

6.1 What Homomorphic Encryption Does

Post-quantum cryptography addresses the threat to data in transit and at rest. Homomorphic Encryption (HE) closes the third and final gap in the data-security triad: protecting data while it is actively being processed. In conventional computing architectures, data must be decrypted before any computation can be performed — creating a plaintext exposure window that represents a persistent attack surface regardless of how strong the surrounding encryption is. HE eliminates this window entirely.

A Homomorphic Encryption scheme is a cryptosystem with a special property: it permits specified algebraic operations — addition, multiplication, and in some schemes arbitrary Boolean logic — to be carried out directly on ciphertext. When the result is subsequently decrypted by the authorized key holder, the output is mathematically identical to the result that would have been obtained by performing the same operations on the original plaintext. At no point during computation is plaintext exposed to the processing environment.

NSA has acknowledged Homomorphic Encryption as a priority privacy-enhancing technology alongside the CNSA 2.0 migration. While HE is not currently mandated by CNSA 2.0 — which focuses on the transition from quantum-vulnerable classical algorithms — the NSA's recognition signals that HE is on a standards trajectory. Organizations building cryptographic architectures for 2030 and beyond should treat HE readiness as a second-order planning requirement: not an immediate migration mandate, but a capability investment that pays dividends as the technology matures.

Two major U.S. government investment programs are directly targeting these barriers:

IARPA HECTOR (Homomorphic Encryption Computing Technology and Operations Research): Focused on advancing HE algorithm efficiency and developing tools that reduce the barrier to HE adoption for non-specialist developers.

DARPA DPRIVE (Data Protection in Virtual Environments): A multi-year program focused on developing hardware accelerators for HE computation, targeting a 5–6 order-of-magnitude performance improvement over software implementations. Phase II awards were issued in 2023–2024, with program milestones targeting practical throughput levels by 2026–2027.

6.2 Scheme Landscape: CKKS, BFV/BGV, and TFHE

This property is not new in concept — the theoretical possibility was described by Craig Gentry in his 2009 doctoral thesis, which demonstrated the first fully homomorphic encryption (FHE) construction. What has changed dramatically in the intervening years is performance: the computational overhead of practical HE has fallen by approximately three orders of magnitude

over the past decade, driven by algorithmic improvements in bootstrapping, noise management, and hardware acceleration.

Current TRL for practical HE implementations sits between 4 and 6, depending on the scheme and use case. CKKS-based ML inference and BFV-based financial computation are approaching TRL 6 in research environments; TFHE gate evaluation is in early pilot deployments. The primary barriers to broader adoption are computational throughput — HE operations remain significantly slower than their plaintext equivalents — and the complexity of parameter selection and noise management. See Table 8 below for Scheme Names.

6.3 Strategic Use Cases

All three families are post-quantum secure by construction: their hardness assumptions rest on variants of the Learning With Errors (LWE) or Ring-LWE problems — the same mathematical foundation underlying ML-KEM and ML-DSA in CNSA 2.0. Organizations migrating to CNSA 2.0 are therefore simultaneously building the mathematical infrastructure upon which HE schemes also depend.

Table 8: Principal Homomorphic Encryption Scheme Families

Scheme	Full Name	Optimized For
CKKS	Cheon-Kim-Kim-Song	Approximate arithmetic over real/complex numbers
BFV / BGV	Brakerski-Fan-Vercauteren / Brakerski-Gentry-Vaikuntanathan	Exact integer arithmetic
TFHE	Fast Fully Homomorphic Encryption over the Torus	Boolean circuit evaluation with fast bootstrapping
Scheme	Full Name	Optimized For

6.4 Maturity, Investment, and Trajectory

HE enables a class of capability that is architecturally impossible under conventional encryption: delegated computation over sensitive data without exposing that data to the computing party. The most strategically significant use cases for defense and intelligence applications include:

Encrypted Database Queries: Analysts can retrieve specific records from an encrypted database without revealing either the query or the result to the database operator, supporting privacy-preserving search over sensitive repositories.

Secure Multi-Party Computation: Multiple organizations can jointly compute over the union of their private datasets — for example, threat intelligence fusion across agency boundaries — without any party revealing its raw data to the others.

Confidential AI Inference: Machine learning models can run inference on encrypted inputs, enabling AI-powered analysis of classified or sensitive data without requiring a secure enclave or trusted execution environment in the processing layer.

Private Cloud Analytics: Encrypted government or contractor data can be processed by cloud infrastructure without the cloud provider — or an adversary who has compromised it — ever seeing plaintext. This directly supports zero-trust data architectures in multi-tenant cloud environments.

7 STRATEGIC RECOMMENDATIONS

The transition to post-quantum cryptography is a multi-year undertaking that demands deliberate planning, cross-functional coordination, and sustained investment. For organizations supporting government and defense missions — including MTSI and its clients — the following actions should be initiated without delay. Critically, the planning horizon for this transition has been compressed significantly: Google's March 2026 announcement of a 2029 PQC migration completion target — informed by its position as the organization with the deepest quantum hardware insight in the commercial sector — means that NIST's 2035 outer bound should no longer be treated as a comfortable planning horizon. Organizations should target 2029–2030 readiness for critical systems.

1. **Conduct a Cryptographic Inventory** — Immediately. Catalog all systems, applications, protocols, and data flows currently using RSA, ECC, DH, and other quantum-vulnerable algorithms. This inventory is the essential first step — you cannot migrate what you have not mapped. Include third-party and embedded systems, which are often overlooked. Given Google's 2029 target and the Gidney research demonstrating a 20-fold reduction in the quantum resources needed to break RSA-2048, the window for completing this inventory is narrower than previously assumed. Organizations that have not begun this cataloging effort are already behind the curve. Inventories should be completed no later than mid-2027 to allow sufficient time for phased migration before the 2029–2030 readiness target.
2. **Prioritize High-Value and Long-Lifecycle Data**. Data that must remain confidential for decades — such as classified information, health records, financial data, and personally identifiable information — is most vulnerable to "harvest now, decrypt later" attacks, in which adversaries capture encrypted traffic today and store it for decryption once quantum capabilities mature. These data categories should be the first targets for migration. The accelerated threat timeline reinforced by Google's announcement makes this prioritization even more urgent: every additional month that high-value data transits networks protected only by classical cryptography increases the volume of ciphertext available for future quantum decryption.
3. **Develop a Phased Migration Plan** — Benchmarked to 2029. Align internal timelines with the CNSA 2.0 roadmap but calibrate urgency against Google's 2029 completion target rather than relying solely on the more permissive government deadlines. Begin with software and firmware signing (2030 exclusive-use deadline) and networking equipment (2026 support deadline). Establish clear milestones, accountable owners, and

testing gates for each migration phase. Migration plans should be structured so that critical and high-priority systems achieve post-quantum readiness by 2029–2030, with full organizational migration completed no later than 2031.

4. **Engage Vendors and Supply Chains**. Require quantum-resistant algorithm support in procurement specifications and vendor assessments. Include CNSA 2.0 compliance requirements in Requests for Proposals (RFPs) and contract vehicles. Verify that COTS and GOTS products on the roadmap support the required algorithms and parameter sets. Vendor engagement should begin immediately, as supply chains will face increasing pressure as more organizations accelerate their migration timelines in response to the compressed threat window.
5. **Adopt Crypto-Agility.** Design systems and architectures that can swap cryptographic algorithms without major re-architecture. Crypto-agility enables smoother transitions as standards evolve, reduces the cost of future migrations, and provides resilience against the possibility that any single algorithm may be found vulnerable. In an environment where threat estimates are compressing faster than anticipated — as the Gidney research demonstrates — crypto-agility is not merely a best practice but an operational necessity.
6. **Invest in Workforce Development.** Train cryptographic and cybersecurity staff on post-quantum algorithms, lattice-based cryptography fundamentals, hash-based signature operations, and NIST's evolving guidance. The talent gap in post-quantum cryptography is real, and early investment in training will yield significant returns during the migration period. Organizations should begin training programs immediately to ensure that qualified personnel are available to execute migration activities within the compressed 2027–2030 implementation window.
7. **Accelerate Migration Timelines to Match Industry Leaders**. Google's March 2026 announcement of a 2029 PQC migration completion target — a full year ahead of NIST's deprecation date for classical algorithms — represents an inflection point for the industry. This target was not set arbitrarily; it reflects Google's direct knowledge of quantum hardware progress from its own Willow chip program and internal threat modeling. Organizations supporting national security missions should benchmark their own timelines against this accelerated posture rather than the more permissive government deadlines. The Gidney research demonstrating a 20-fold reduction in the quantum resources needed to break RSA-2048 confirms that threat estimates are compressing faster than anticipated and that earlier assumptions about "decades away" timelines are no longer defensible. MTSI recommends that clients treat 2029 as a functional planning deadline for critical systems, with full migration completed no later than 2031. Any organization whose current roadmap targets 2035 readiness should immediately reassess and compress its timeline accordingly.

Monitor and Pilot Homomorphic Encryption. While HE is not yet a mandated standard, its maturity trajectory and strategic relevance to defense and intelligence missions warrant proactive engagement. Organizations should designate a technical working group to track DARPA DPRIVE and IARPA HECTOR program outcomes, evaluate open-source HE libraries (including Microsoft SEAL, OpenFHE, and Google's FHE Transpiler) against candidate use cases, and identify one or two internal pilot applications — such as encrypted analytics over sensitive datasets or private ML inference — where HE could be validated at low operational risk. Early investment in HE fluency will position organizations to adopt the technology efficiently as it crosses the TRL 7 threshold and enters standardization consideration.

8 CONCLUSION

The data protection landscape relies on a multi-layered approach using symmetric, asymmetric, and hybrid encryption. While established algorithms like AES and RSA are cornerstones of data security, the industry is proactively preparing for the future threat of quantum computing with the development and transition to quantum-resistant cryptography, as outlined in the CNSA 2.0 suite.

The threat is neither hypothetical nor distant. The NSA's CNSA 2.0 timeline reflects an institutional assessment that the window for safe migration is finite — and narrowing. Web browsers and cloud services were expected to begin supporting quantum-resistant algorithms by 2025; networking equipment must follow by 2026; and exclusive use of CNSA 2.0 algorithms for software and firmware signing is mandated by 2030. Organizations that have not begun their transition are not merely behind schedule — they are accumulating risk with every day that quantum-vulnerable algorithms protect sensitive data.

The urgency of this transition was underscored in March 2026 when Google — the company simultaneously building one of the world's most advanced quantum computers and operating critical global internet infrastructure — announced a hard 2029 deadline to complete its own post-quantum migration. With the Gidney research demonstrating that the quantum resources required to break RSA-2048 have collapsed by a factor of twenty in just six years, the threat horizon is compressing faster than even optimistic projections anticipated. Organizations that delay action risk finding themselves exposed not in 2035, but years earlier.

The good news is that the cryptographic tools for the post-quantum era are available today. ML-KEM, ML-DSA, LMS, and XMSS have been standardized by NIST, and commercial implementations are maturing. The path forward requires not breakthrough research but disciplined execution: inventorying cryptographic dependencies, prioritizing high-value data, building phased migration plans, and investing in the workforce that will carry those plans to completion. Looking further ahead, Homomorphic Encryption is advancing from research prototype to operational pilot, offering a path to computation over ciphertext that will complete the zero-trust data-protection triad — securing data in transit, at rest, and in use.

REFERENCES

The following sources informed the analysis, technical specifications, and strategic recommendations presented in this white paper.

8.1.1 Government Standards and Policies

[1] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES).* NIST, November 26, 2001. https://doi.org/10.6028/NIST.FIPS.197

[2] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.* NIST, August 13, 2024. https://doi.org/10.6028/NIST.FIPS.203

[3] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 204: Module-Lattice-Based Digital Signature Standard.* NIST, August 13, 2024. https://doi.org/10.6028/NIST.FIPS.204

[4] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 205: Stateless Hash-Based Digital Signature Standard.* NIST, August 13, 2024. https://doi.org/10.6028/NIST.FIPS.205

[5] National Institute of Standards and Technology (NIST). *Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes.* NIST, October 2020. https://doi.org/10.6028/NIST.SP.800-208

[6] National Institute of Standards and Technology (NIST). *Announcing Issuance of Federal Information Processing Standards (FIPS) 203, 204, and 205.* Federal Register, Vol. 89, No. 157, pp. 66052–66056, August 14, 2024.

[7] National Security Agency (NSA). *Commercial National Security Algorithm Suite 2.0.* Cybersecurity Advisory, September 7, 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[8] National Security Agency (NSA). *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ.* Cybersecurity Information Sheet, November 2022. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

[9] National Security Agency (NSA). *NSA Suite B Cryptography.* Committee on National Security Systems Policy No. 15 (CNSSP-15), Annex B, originally published February 16, 2005; updated October 2012.

[10] Committee on National Security Systems (CNSS). *CNSS Policy No. 15, Fact Sheet No. 1: National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information.* CNSS, June 2003.

8.1.2 Academic and Research Publications

[11] Shor, P.W. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring.* Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Society Press, pp. 124–134, November 1994. https://doi.org/10.1109/SFCS.1994.365700

[12] Shor, P.W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM Journal on Computing, Vol. 26, No. 5, pp. 1484–1509, October 1997. arXiv:quant-ph/9508027.

[13] Grover, L.K. *A Fast Quantum Mechanical Algorithm for Database Search.* Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), Philadelphia, PA, pp. 212–219, May 1996. arXiv:quant-ph/9605043.

[14] Gidney, C. *How to Factor 2048-Bit RSA Integers with Less Than a Million Noisy Qubits.* arXiv preprint, arXiv:2505.15917 [quant-ph], May 21, 2025. https://doi.org/10.48550/arXiv.2505.15917

[15] Gidney, C. and Ekerå, M. *How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits.* Quantum, Vol. 5, p. 433, April 2021. arXiv:1905.09749.

[16] Google Quantum AI and Collaborators. *Quantum Error Correction Below the Surface Code Threshold.* Nature, Vol. 636, pp. 920–926, December 2024. https://doi.org/10.1038/s41586-024-08449-y

8.1.3 Industry Publications

[17] Adkins, H. and Schmieg, S. *Quantum Frontiers May Be Closer Than They Appear.* The Keyword (Google Blog), March 25, 2026. https://blog.google/technology/safety-security/quantum-frontiers-may-be-closer-than-they-appear/

[18] Neven, H. *Meet Willow, Our State-of-the-Art Quantum Chip.* The Keyword (Google Blog), December 9, 2024. https://blog.google/technology/research/google-willow-quantum-chip/

[19] Castelvecchi, D. *"A Truly Remarkable Breakthrough": Google's New Quantum Chip Achieves Accuracy Milestone.* Nature News, Vol. 636, pp. 527–528, December 9, 2024. https://doi.org/10.1038/d41586-024-04028-3

[20] Google Just Drew a Line in the Sand: PQC Migration by 2029 - Postquantum

[21] Google Moves Q Day to 2029: Quantum Computing Breaks Encryption - MachineEra

[22] Google bumps up Q Day deadline to 2029, far sooner than previously thought - Ars Technica

[23] Google sets 2029 deadline for quantum-safe encryption, years ahead of government targets | TechSpot

[24] STIG-Consulting, Enterprise Transformation and Governance PQC; QUANTUM RISK: A 2026 Global Doctrine for Post-Quantum Cryptography Migration, Board Accountability and Cryptographic Solvency, White Papers for PQC written by Brian Couzens; https://www.sitg-consulting.com/white-papers.

8.1.4 Homomorphic Encryption

[24] Gentry, C. A Fully Homomorphic Encryption Scheme. Ph.D. Dissertation, Stanford University, 2009. https://crypto.stanford.edu/craig/craig-thesis.pdf

[25] Cheon, J.H., Kim, A., Kim, M., and Song, Y. Homomorphic Encryption for Arithmetic of Approximate Numbers. Advances in Cryptology — ASIACRYPT 2017, Lecture Notes in Computer Science, Vol. 10624, Springer, pp. 409–437, 2017. https://doi.org/10.1007/978-3-319-70694-8_15

[26] Defense Advanced Research Projects Agency (DARPA). Data Protection in Virtual Environments (DPRIVE) Program. DARPA Information Innovation Office (I2O). https://www.darpa.mil/program/data-protection-in-virtual-environments

[27] Microsoft Research. Microsoft SEAL: Simple Encrypted Arithmetic Library. Version 4.x. https://github.com/microsoft/SEAL

[28] OpenFHE Development Team. OpenFHE: Open-Source Fully Homomorphic Encryption Library. https://www.openfhe.org/