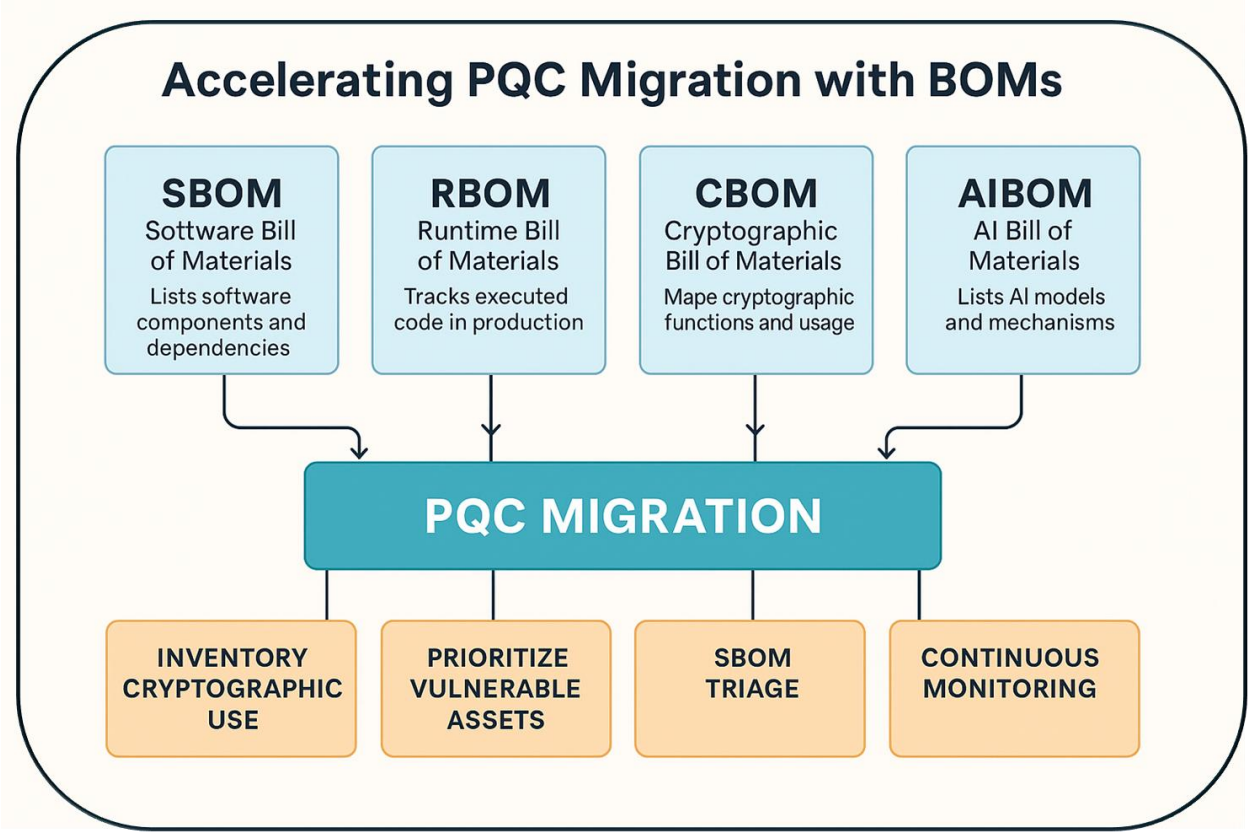
Accelerating Enterprise Post-Quantum Cryptography Migration by Using BOMs (Software, Release, Cryptographic, and AI Bills of Materials) and Hardware / Software products.



Contact:

Thomas Bronack, President

Data Center Assistance Group, LLC

bronackt@dcag.com

(917) 673-6992

Table of Contents

Contents

Accelerating Enterprise Migration to Post-Quantum Cryptography Using Software, Release, Cryptographic, and AI Bills of Materials

Executive Summary:

As quantum computing advances, today's widely used encryption algorithms face obsolescence due to their vulnerability to quantum attacks from algorithms like Shor's (Prime Number Factoring) and Grover's (Brute Force Decryption) algorithms. Enterprises must prepare now for this cryptographic disruption. This white paper provides an actionable framework for reducing discovery time and accelerating Post-Quantum Cryptography (PQC) migration by integrating Software Bill of Materials (SBOMs), Release BOMs (RBOMs), Cryptographic BOMs (CBOMs), and AI BOMs (AIBOMs). These assets offer visibility into cryptographic use, enabling efficient detection, prioritization, and mitigation of quantum vulnerabilities.

Current problems already exist through the practice of Harvest-Now-Decrypt-Later (HNDL) which copies encrypted software and data off-site and stored until Quantum Computers can decrypt the data. At that point, the data will be for sale or usage through the dark web.

Once your data exposure becomes known, your company brand and reputation will suffer, clients will leave, compliance penalties applied, and clients will depart.

Do you know how exposed you already are? This means your data is already at risk and you may not know it. Once stolen your data will not be recoverable, because the data can be decrypted off-site after it has been harvested.

Section 1: The Cryptographic Landscape Today

Encryption Algorithms and Key Management Challenges			
Algorithm:	Type:	Estimated Usage:	Key Management Challenges:
RSA	Symmetric	~85%	Complex distribution at scale
ECC	Asymmetric	~60%	Long key lengths, costly operation
3DES	Symmetric	<5%	Curve selection complexity, compatibility issue
DH	Key Exchang	~30%	Curve selection complexity, compatibility issue

Most encryption methods rely on difficult mathematical problems (e.g., factoring large primes) that quantum computers can solve exponentially faster than classical computers.

Section 2: Quantum Threats to Classical Encryption

- Shor's Algorithm can efficiently factor large numbers and compute discrete logarithms, breaking RSA and ECC.

- Grover's Algorithm reduces the complexity of brute-forcing symmetric keys by half.

Comparative Times to Crack an Encrypted Password - Classical Computer vs Quantum Computer		
Password Length:	Classical Attack Time:	Quantum Attack Time:
8 Characters	Hours	Seconds
10 Characters	Weeks	Minutes
12 Characters	Years	Hours
14 Characters	Centuries	Days
16 Characters	Millenia	Weeks

Decryption Times with Quantum Computers vs Classical Computers

Time Required to Decrypt a Password using Classical Computers as compared to Quantum Computers				
Password Length	Charset	Classical Time	Quantum (Grover's)	Quantum (Grover's + Shor's)
6	Alphanumeric + Symbols	12.25 minutes	0.00 sec	1.00 seconds
7	Alphanumeric + Symbols	19.40 hours	0.01 sec	1.01 seconds
8	Alphanumeric + Symbols	10.97 weeks	0.08 sec	1.08 seconds
9	Alphanumeric + Symbols	19.97 years	0.79 sec	1.79 seconds
10	Alphanumeric + Symbols	18.97 centuries	7.74 seconds	8.74 seconds
11	Alphanumeric + Symbols	1802.42 centuries	1.26 minutes	2.26 seconds
12	Alphanumeric + Symbols	171229.78 centuries	12.25 minutes	13.25 seconds
13	Alphanumeric + Symbols	16266829.01 centuries	1.99 hours	2.99 seconds
14	Alphanumeric + Symbols	1545348756.29 centuries	19.40 hours	20.40 seconds
15	Alphanumeric + Symbols	146808131847.72 centuries	1.13 weeks	2.13 seconds
16	Alphanumeric + Symbols	13946772525533.18 centuries	10.97 weeks	11.97 seconds
17	Alphanumeric + Symbols	1324943389925651.50 centuries	2.05 years	3.05 seconds
18	Alphanumeric + Symbols	125869622042936880.00 centuries	19.97 years	20.97 seconds
19	Alphanumeric + Symbols	11957614094079006720.00 centuries	1.95 centuries	2.95 seconds
20	Alphanumeric + Symbols	1135973338937505480704.00 centuries	18.97 centuries	19.97 seconds

These threats underscore the need for rapid cryptographic modernization.

Section 3: Challenges in Identifying Encryption Usage

Locating and mapping the use of cryptography across a large enterprise is traditionally resource intensive. Encryption is embedded in:

- Applications (via OpenSSL, Java libraries)
- Network communications (TLS)
- Storage (BitLocker, TDE)
- Email systems (S/MIME, PGP)
- Cloud services (KMS, Vault)
- Identity & Access Management (PKI)

Manual audits and legacy scans often fail to detect all cryptographic endpoints, especially in CI/CD pipelines and microservices.

Section 4: The BOM-Based Acceleration Model

- **SBOM** (Software Bill of Materials)
  - Lists of all software components and libraries
  - Detects outdated cryptographic libraries.
  - Detects vulnerabilities and provides update paths.
- **RBOM** (Release Bill of Materials)
  - Tracks which software components are running in production.
  - Helps focus mitigation efforts only on in-use components.

- **CBOM** (Cryptographic Bill of Materials)
  - Maps where and how cryptographic algorithms are used.
  - Directly identifies quantum-vulnerable cryptographic dependencies.
- **AIBOM** (AI Bill of Materials)
  - Identifies AI systems relying on cryptography.
  - Ensure secure decision-making in AI pipelines.

Section 5: Tasks Accelerated by BOM Integration

Use of BOMs to accelerate Post Quantum Migration Tasks		
Task:	BOM:	Contribution:
Inventory	CBOM	Enables Rapid Visibility
Prioritize Assets	RBOM	Higlights Active Usage of Assets
SBOM Triage	SBOM Triage	Focus on Open-Source or Third-Party vulnerabilities
Continuous Monitoring	SBOM, RBOM	Real-Time updates and alerts via BOM platforms

Integrating BOMs reduces discovery time by 60–80%, supports regulatory compliance (e.g., NIST SP 800-208), and enables faster, more accurate PQC decision-making.

Section 6: Next Steps for Enterprise Readiness

1. Inventory cryptographic assets using SBOM/CBOM tools

2. Triage live systems with RBOM prioritization

3. Apply PQC algorithms (e.g., CRYSTALS-Kyber) as hybrid solutions

4. Monitor AI systems with AIBOM and CBOM integrations

5. Ensure compliance with federal mandates (e.g., NSA CNSA 2.0, EO 14028)

CNSA Suite 2.0

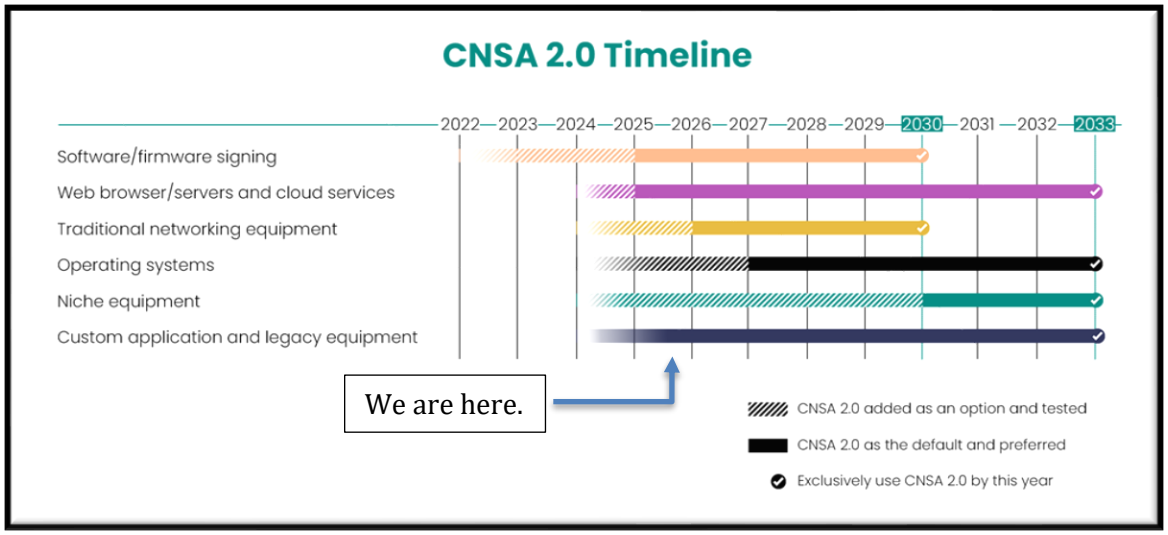
Post-Quantum Cryptography Algorithms

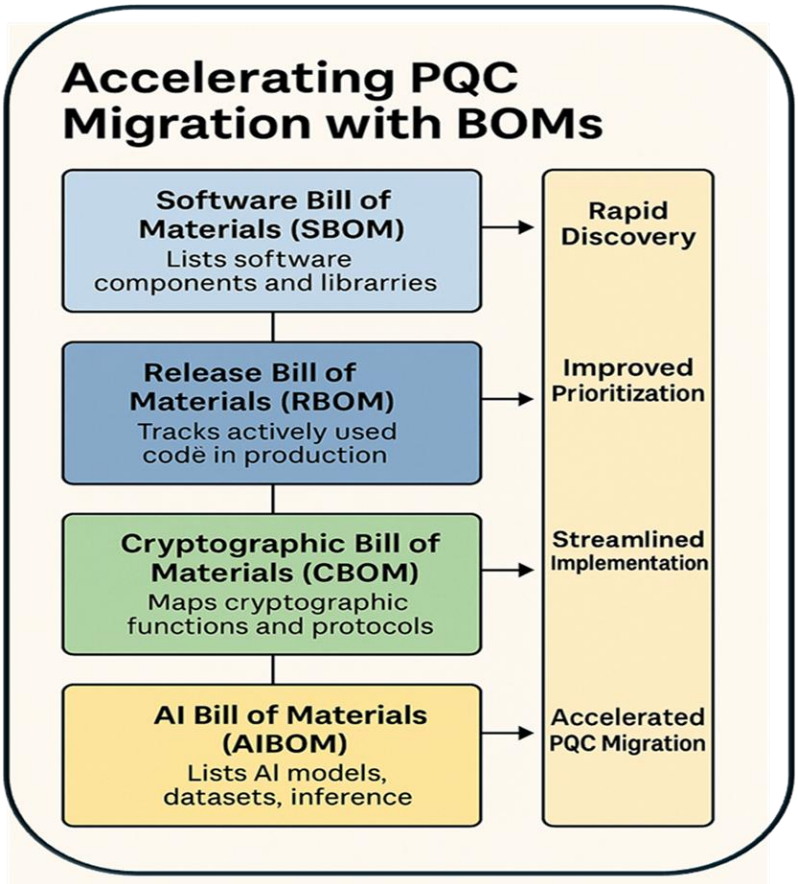
NSA has announced its selections for quantum-resistant algorithms. Please see CNSS Policy 15, released March 4, 2025, and the FAQ for the Commercial National Security Algorithm (CNSA) Suite 2.0 for details.

Conclusion

PQC migration is not just a cryptographic upgrade—it is a business imperative. BOM-driven intelligence enables enterprises to fast-track risk identification, prioritize critical assets, and implement resilient, quantum-safe encryption before the quantum threat becomes reality.

Visual Reference: See "Accelerating PQC Migration with BOMs" flowchart (included).





References

- NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes

- NSA CNSA 2.0 Algorithm Suite Guidance

- NIST PQC Standardization Process Finalists: https://csrc.nist.gov/projects/post-quantum-cryptography

Call to Action

Contact us to further discuss how we can help you migrate to Post Quantum Computing (PQC) and Future-Proof your enterprise.

Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com, or bronackt@gmail.com
(917) 673-6992