WHITE PAPER

Cryptographic Bill of Materials for Executive Order 14412

Producing verifiable evidence of cryptographic posture before the standard that will grade it exists.

A practical framework for federal contractors, security teams, and compliance leaders.

NextGenRails™

cbomcompliance.com

July 2026 · Protocol NGR-TEC-CBM-002 · Ruleset NGR-CBOM-QRS-2026.07.3

Executive Summary

Executive Order 14412, signed 22 June 2026, puts federal cryptography on a clock. High Value Assets and high-impact systems must move to post-quantum key establishment by 31 December 2030, and to post-quantum digital signatures by 31 December 2031. A proposed FAR rule, due within 180 days of the order, will pull covered contractors onto the same timeline. OMB memorandum M-26-15, issued two days after the order, requires every federal civilian agency to submit a post-quantum migration plan within 120 days.

The order also directs CISA and NIST to publish the minimum elements of a Cryptographic Bill of Materials within 270 days — expected around March 2027. That creates an awkward gap, and the gap is what this paper is about.

THE PROBLEM, STATED PLAINLY

> Nobody can certify a CBOM against a specification that has not been published yet. Any vendor claiming to certify your CBOM as *EO 14412 compliant* today is selling you something that cannot exist.
>
> But §5(d) of the order tells you what the CBOM is *for*: automated assessment. That requirement is testable now. A cryptographic inventory either supports automated assessment or it does not — and you can find out today, while there is still time to fix what is missing.

NextGenRails™ CBOM Compliance tests exactly that. It reads an existing CycloneDX or SPDX manifest, extracts and grades every cryptographic asset against NIST guidance, maps each quantum-vulnerable finding to the EO 14412 deadline that actually applies to it, and evaluates the inventory against ten versioned conformance rules derived from the order's functional requirement and from NIST IR 8547.

The check is free and uncapped. Where durable evidence is needed, the platform issues a receipt: a signed, independently verifiable record of what an inventory contained and how it graded, at a moment in time. Receipts are signed twice — with RS256 for the tooling that exists today, and with ML-DSA-65 (FIPS 204) for the decade in which RSA does not.

This paper states what the order requires, what the platform does, and — in Section 6 — what it does not do. That last section is not a disclaimer. It is the reason to trust the rest.

1 What EO 14412 Actually Requires

Precision matters here, because several published summaries of this order are wrong. The following is drawn from the text as published in the Federal Register, 91 FR 38483, 25 June 2026.

1.1 The clock

DEADLINE	SECTION	REQUIREMENT
30 days 22 Jul 2026	§4(a)	Each agency head identifies its PQC migration lead and provides the name and contact details to OMB and the National Cyber Director. **This is a naming requirement. No inventory is due at 30 days.**
90 days 20 Sep 2026	§4(b)	OMB issues guidance requiring agencies to review their inventory of HVAs and high-impact systems, transition those systems by the 2030 and 2031 dates, and submit a plan.
180 days 19 Dec 2026	§5(c)	The FAR Council publishes a proposed rule requiring covered contractors to comply with NIST FIPS, including PQC-compliant FIPS, by 31 December 2030.
180 days	§5(b)	NIST revises the Cryptographic Module Validation Program to accelerate validation of cryptographic modules.
270 days ~Mar 2027	§5(d)	CISA and NIST publish guidance on the minimum elements for a Cryptographic Bill of Materials.
31 Dec 2030	§4(b)(ii)	HVAs and high-impact systems use PQC for key establishment.
31 Dec 2031	§4(b)(iii)	HVAs and high-impact systems use PQC for digital signatures.

Two points of scope are commonly misreported. First, the 2030 and 2031 deadlines apply to High Value Assets and high-impact systems, *excluding National Security Systems* — not to every system an agency operates. Second, the 30-day requirement is to name a person, not to produce an inventory. Any material telling you otherwise — particularly material from a vendor selling inventory tooling — should be read with that in mind.

1.2 The memorandum that starts the work: OMB M-26-15

On 24 June 2026 — two days after the order, well inside the 90-day window it allowed — OMB issued M-26-15, *Execution of the Migration to Post-Quantum Cryptography*. It operationalises the executive order on top of the existing M-23-02 requirements.

The hard requirement: every federal civilian agency must submit a PQC migration plan to OMB and the Office of the National Cyber Director **within 120 days**, aligned to NIST IR 8547, spanning five phases through 2035. The headline 2030 and 2031 dates are the priority-system deadlines. 2035 is the backstop for everything else.

For contractors, the practical consequence is this: your customers' plans are due around late October 2026, and those plans have to describe a supply chain. **You will be asked what cryptography is in your software before the CBOM standard exists.**

1.3 The standard that will grade you: NIST IR 8547

EO 14412 sets the dates. NIST IR 8547 sets the technical criteria, and M-26-15 aligns agency planning to it explicitly. Its transition schedule is what an inventory will actually be judged against.

ALGORITHM CLASS	DEPRECATED	DISALLOWED
RSA at 112-bit security (e.g. RSA-2048)	2030	2035
ECDSA / ECDH (P-256 and equivalent)	2030	2035
Finite-field DH / DSA (112-bit)	2030	2035
Below 112-bit security (RSA-1024, 3DES, SHA-1)	**Already deprecated**	**Already disallowed**

This distinction is what separates a cryptographic inventory from a list of libraries. An RSA-2048 key used for *key establishment* is a 2030 problem. The same key used for a *digital signature* is a 2031 problem. An RSA-1024 key is not a future problem at all — it is a present failure. An inventory that cannot tell those three cases apart cannot support automated assessment, and therefore cannot satisfy §5(d), whatever the minimum elements eventually say.

1.4 Why an SBOM will not do this

Most organisations already hold SBOMs produced by Syft, Trivy, cdxgen or a build-system plugin. They are genuinely useful for software composition analysis. They are not cryptographic inventories.

- They enumerate *components*, not cryptographic assets. An SBOM lists `openssl 3.0.11`. It does not tell you which algorithms, key sizes and usage contexts that library actually exposes in your deployment.
- They carry no machine-readable declaration of primitive, key size, or usage — the

three fields on which every EO 14412 deadline turns.

- They carry no cryptographic binding, so a third party cannot verify that the SBOM they were handed is the SBOM you produced.
- They map to no deadline and produce no risk grade, so they cannot be assessed automatically — which is the one thing §5(d) requires of a CBOM.

The gap is not that SBOMs are deficient. It is that they answer a different question.

2 Verifiable CBOM Receipts

The platform does two things, and it is worth being clear that they are separate.

2.1 The check — free, uncapped, no account

Upload a CycloneDX 1.6 or 1.7 (ECMA-424) or SPDX JSON manifest. The system extracts cryptographic assets, resolves what each one is *used for*, grades it against NIST guidance, assigns every quantum-vulnerable finding to the EO 14412 deadline that actually applies to it, and evaluates the inventory against ten versioned CBOM conformance rules.

You get a full assessment: what is broken now, what breaks in 2030, what breaks in 2031, and where the inventory falls short of supporting automated assessment. No account, no email, no payment, no limit. The manifest is processed in memory and discarded.

This is the part that tells you something you did not already know. **It costs nothing, and it always will.**

2.2 The receipt — durable, signed, independently verifiable

A check tells you the state of an inventory. A receipt lets you prove that state to somebody else, later, without their having to trust you — or us.

A receipt is a JWS containing the assessment, a SHA-384 fingerprint of the submitted manifest, and a Merkle root computed over normalised component data. It is signed twice.

SIGNATURE	ALGORITHM	WHY
Classical	RS256 (RSA, PKCS#1 v1.5, SHA-256)	Verifiable today by any standard JWS library, in any language, with no special tooling.
Post-quantum	ML-DSA-65 (FIPS 204)	Remains meaningful after RSA does not. A 3,309-byte detached signature over the identical signing input.

Both signatures cover the same bytes. A verifier who trusts only one of them still holds a complete proof.

This matters more than it sounds. A tool that warns you about RSA, and then signs that warning with RSA alone, has produced evidence that expires on the same schedule as the problem it describes. **The receipt is signed with the algorithm it is telling you to migrate to.**

3 How It Works

1. **Upload.** Submit a CycloneDX 1.6 or 1.7 (ECMA-424) or SPDX JSON manifest. No account required.
2. **Analyse.** Cryptographic assets are extracted and classified by primitive, key size and usage context, then graded against NIST guidance and the IR 8547 transition dates.
3. **Assess.** The inventory is evaluated against ten versioned conformance rules. The result states whether the inventory is *machine-assessable* — not whether it is *certified*. See Section 6.
4. **Fingerprint.** A SHA-384 hash of the submitted manifest and a Merkle root over normalised component data are computed.
5. **Sign.** The payload is signed with RS256 and co-signed with ML-DSA-65. If post-quantum co-signing fails for any reason, the declaration is stripped and the receipt re-signed — *a receipt cannot claim a signature it does not carry*.
6. **Deliver.** The signed receipt is returned immediately. The manifest is discarded.

3.1 Verification

Any party can verify a receipt against the published keyset. Verification requires no account, no payment, and no contact with NextGenRails. The keyset contains every key ever used — active and retired — with its validity window, so a receipt issued years

ago still verifies after the signing key has rotated.

Cache the keyset, and verification works entirely offline. This is the property that matters for audit evidence: **your ability to prove what you submitted must not depend on our continued existence.**

4 The Conformance Ruleset

Ten versioned rules, published with each receipt and identified by ruleset version, so a receipt issued today can be re-checked against the rules that were in force when it was issued. The rules test one thing: whether an inventory supports automated cryptographic assessment, as §5(d) requires.

4.1 The distinction the whole assessment turns on

Under EO 14412, the deadline that applies to an algorithm depends on what it is *used for*, not what it is.

ALGORITHM FAMILY	PRIMITIVE	DEADLINE UNDER EO 14412
RSAES-OAEP RSAES-PKCS1	pke	**31 Dec 2030 — key establishment**
RSASSA-PKCS1 RSASSA-PSS	signature	**31 Dec 2031 — digital signatures**

The same modulus. The same key length. One year apart. And nothing in the component name reliably distinguishes them — both are routinely emitted as `RSA-2048`.

This is not a corner case. It is the central mechanical problem of grading a CBOM, and an inventory that cannot express the difference cannot be assessed automatically, whatever the minimum elements eventually say.

4.2 The CycloneDX Cryptography Registry

CycloneDX v1.7 (October 2025) introduced the **Cryptography Registry**: an authoritative, machine-readable set of algorithm families and elliptic curves, published because inconsistent algorithm naming across tools was breaking PQC readiness assessments in exactly this way. It also added `algorithmProperties.algorithmFamily`.

The registry is what makes deadline assignment mechanizable rather than heuristic. This platform resolves the usage of every asset in strict order of trustworthiness:

1. The declared `primitive`. The issuer said so explicitly.
2. `algorithmFamily`, resolved through the CycloneDX Cryptography Registry. The standard says so.
3. `cryptoFunctions`. Inferred from the operations the asset actually performs.
4. Unknown — flagged, and assigned the *earliest* applicable deadline rather than a convenient one.

At no point is the usage guessed from the component's name. A free-text name is not a declaration, and grading a regulated deadline off a regex over a string somebody typed is not an assessment.

4.3 What the rules test

- Whether cryptographic assets are distinguishable from ordinary software components at all.
- Whether each asset declares its primitive — or an `algorithmFamily` the registry can resolve.
- Whether key size or security strength is declared. Without it, RSA-1024 and RSA-3072 are the same entry.
- Whether usage context is declared. This is the difference between a 2030 deadline and a 2031 one.
- Whether certificates carry issuer, subject, validity window and signature algorithm.
- Whether protocol versions are pinned, so that a TLS entry means something.

An inventory that passes is not *EO 14412 certified*. No such thing exists yet. It is an inventory a machine can grade — which is the prerequisite for every certification that will exist, and the thing that can be fixed now rather than in March 2027.

5 Who This Is For

ROLE	WHAT IT GIVES THEM
PQC migration leads named under §4(a)	A prioritised view of quantum-vulnerable assets across the portfolio, sorted by the deadline that applies to each — the inventory the role was created to own.
Federal contractors and subcontractors	Preparation for the proposed FAR rule due December 2026, and an answer when a prime asks what cryptography ships in your software.
Security and compliance teams	Evidence that can be handed to an auditor and verified without trusting the vendor who produced it.
Software vendors	Signed composition attestations that customers can verify independently, including after a release has shipped.

Common use cases: pre-deployment cryptographic risk assessment; validating a vendor-supplied SBOM and detecting substitution; assembling audit evidence for CMMC, FedRAMP or the EU Cyber Resilience Act; and proving, after a migration, that the quantum-vulnerable assets are actually gone.

6 What This Does Not Do

Every vendor in this category will tell you what their product does. Here is what ours does not. If any of the following is a dealbreaker, we would rather you discovered it now than in an audit.

READ THIS BEFORE RELYING ON A RECEIPT

> A receipt is evidence of *what was submitted* and *how it graded*. It is not a certification, and it is not a statement about software you own.

A CLAIM WE DO NOT MAKE	WHAT IS ACTUALLY TRUE
It certifies EO 14412 compliance	It cannot. CISA and NIST have not published the minimum CBOM elements (§5(d), due ~March 2027). Nothing can be certified against an unpublished specification. What the platform tests is the order's *functional* requirement: whether an inventory supports automated assessment.
It proves you own the software	It does not. A receipt attests that a particular manifest was submitted and graded at a particular time. It makes no claim about who owns, controls or ships the software described. Anyone can submit any manifest.
The keys are hardware-backed	They are not. Signing keys are generated in-process and held in encrypted cloud storage, not in an HSM. The threat model is that the key store and its credentials are protected — not that the private key was never extractable. This is stated in the public keyset endpoint.
Receipts are anchored to a blockchain	They are not. No receipt is committed to any public ledger. A receipt's integrity rests on its two signatures and on the published key history — which is sufficient, and which we would rather state plainly than dress up.
It scans your code	It does not. It reads the manifest you provide. If your SBOM omits a cryptographic dependency, the receipt will faithfully record an inventory that omits it.
Trial receipts are audit evidence	They are not, and they say so in the signed payload. Free receipts carry an unstrippable trial marking. They exist so the mechanism can be verified end-to-end before anything is paid for.

6.1 Two disclosures about the platform itself

Consistency requires that we hold ourselves to the standard we are grading you against.

- **The classical signing key is currently RSA-2048.** Under NIST IR 8547 that is acceptable today and deprecated by 2030 — precisely the finding the platform would report about your inventory. It is scheduled for rotation to RSA-3072, and the active key size is published in the keyset endpoint at all times. This is also exactly why every receipt is co-signed with ML-DSA-65: the post-quantum signature is not a marketing feature. It is the one that still means something in 2032.
- **Receipts issued before 13 July 2026 may carry a misleading *explanation* of a correct deadline.** Under ruleset NGR-CBOM-QRS-2026.07.2, the key-establishment test omitted the `pke` primitive. An asset that correctly declared RSA key transport

was recorded as having no declared primitive, and so reached the 2030 deadline through the fallback path rather than by reasoning. The deadline was right; the stated basis for it was not. Fixed in ruleset 2026.07.3, which also adopts the CycloneDX Cryptography Registry. Ruleset versions are pinned into every receipt precisely so that a change like this is visible rather than silent.

- **Receipts issued before 12 July 2026 may declare a post-quantum co-signature that was never produced**, owing to a defect in the signing path. Their RS256 signatures are unaffected and remain valid. The public verifier flags affected receipts explicitly rather than silently passing them. Receipts issued after that date cannot declare a signature they do not carry.

7 Access and Pricing

TIER	PRICE	WHAT IT INCLUDES
Free check	Free, uncapped	Unlimited cryptographic inventory analysis, deadline mapping and conformance assessment. No account. No receipt.
Free receipts	Free	Up to three signed receipts per IP per day, standard tier, carrying an unstrippable trial marking. Subject to a global daily ceiling.
Standard pack	$49 once	Ten signed receipts, full cryptographic proof, no trial marking. *Does not include comparison or re-evaluation.*
Advanced pack	$199 once	Ten signed receipts including vulnerability intelligence, component-level risk analysis, receipt comparison (drift detection) and time-aware re-evaluation.
Professional	$299 / month	Higher volume, standard-tier receipts. Comparison and re-evaluation are Advanced-tier features and are *not* included.
Professional Plus	$999 / month	Higher volume, Advanced-tier receipts, including comparison and re-evaluation.
Enterprise	Contract	Volume licensing and custom terms.

WHICH FEATURES ARE TIER-GATED, STATED ONCE

> Receipt comparison — drift detection between two receipts — and time-aware re-evaluation require **Advanced-tier** receipts. A Standard receipt cannot be compared or re-evaluated. If those capabilities are the reason you are buying, buy Advanced.

8 Getting Started

1. Go to `cbomcompliance.com` and upload a CycloneDX or SPDX manifest. No account. Nothing to install.
2. Read the assessment: what is already non-compliant, what expires in 2030, what expires in 2031, and where the inventory fails to support automated assessment.
3. Fix the inventory. This is the actual work, and it is the reason to start now rather than in 2027.
4. Issue a receipt when durable evidence is needed — for a prime, an auditor, or an internal governance record.
5. Verify it yourself against the public keyset before relying on it. It takes about four minutes, and you should not take our word for any of this.

Conclusion

The 270-day gap is real, and it is already being filled by vendors selling certification against a specification that does not exist. That is not caution talking — it is arithmetic. CISA and NIST publish the minimum CBOM elements around March 2027. Nothing before then can be certified against them.

What *can* be done now is the part that actually takes time: making an inventory good enough to be graded by a machine. Organisations that do that will spend 2027 producing evidence. Those that wait will spend 2027 discovering that they never had an accurate picture of their own cryptography, with three years left on a nine-year problem.

The check is free, and it will tell you where you stand today. **Everything else in this document is optional.**

Contact

Website · `cbomcompliance.com`

Verification · `cbomcompliance.com/verify.html`

Public keyset · `cbomcompliance.com/.netlify/functions/public-key`

Enterprise · `ngr.admin@proton.me`

Regulatory citations in this paper are drawn from Executive Order 14412 as published at 91 FR 38483 (25 June 2026), OMB memorandum M-26-15 (24 June 2026), and NIST IR 8547. Cryptographic asset modelling follows CycloneDX v1.6/v1.7 (ECMA-424) and the CycloneDX Cryptography Registry. Where this paper describes the platform's own limitations, those statements are reproduced from the live service and can be checked against it.