NETRISE

Guidance for Federal Agencies

# Why PQC Readiness Starts with Cryptographic Visibility


Recent research from Google adds to a growing body of evidence that federal agencies should treat post-quantum cryptography (PQC) readiness as an immediate planning and inventory priority, not a distant modernization exercise. Google's latest work shows that advances in quantum hardware and algorithm construction are reducing the quantum resources needed to break elliptic curve cryptography, one of the foundations of modern digital trust.

At the same time, security leaders such as Phil Venables have emphasized that the central challenge is not simply the eventual arrival of cryptanalytically relevant quantum computers, but the length and complexity of the migration itself. Organizations that have not yet begun identifying where cryptography exists in their environments may already be behind.

For federal agencies, the message is clear:

**PQC readiness should be treated as an enterprise visibility, prioritization, and modernization problem now.**

# Why this Matters to Agencies Now

The most important takeaway from the latest quantum research is not just that the threat is real. It is that the planning window is narrowing. Google's updated estimates show meaningful reductions in the qubits and gates required to attack ECDLP-256, continuing a trend of steady improvement in the practical feasibility of quantum cryptanalysis.

For agencies, that creates two immediate concerns.

First, migration timelines are long. Federal environments are large, heterogeneous, and dependent on legacy systems, embedded technologies, vendors, integrators, and mission platforms with long refresh cycles. Venables notes that crypto migration must extend well beyond core toolkits to include communications protocols, middleware, authentication services, software signing, applications, supply chain dependencies, and hardware. That sounds less like a software patch and more like a government-wide renovation with the walls still occupied.

Second, adversaries do not operate on federal procurement timelines. Even when broad migration policy is clear, agencies still have to discover where vulnerable cryptography exists, determine mission impact, set priorities, and coordinate with suppliers and downstream stakeholders. That work cannot begin in earnest without visibility.

**The most important takeaway from the latest quantum research is not just that the thread is real. It is that the planning window is narrowing.**

*Google's Quantum Computer*

# The first requirement is not replacement. It is discovery.

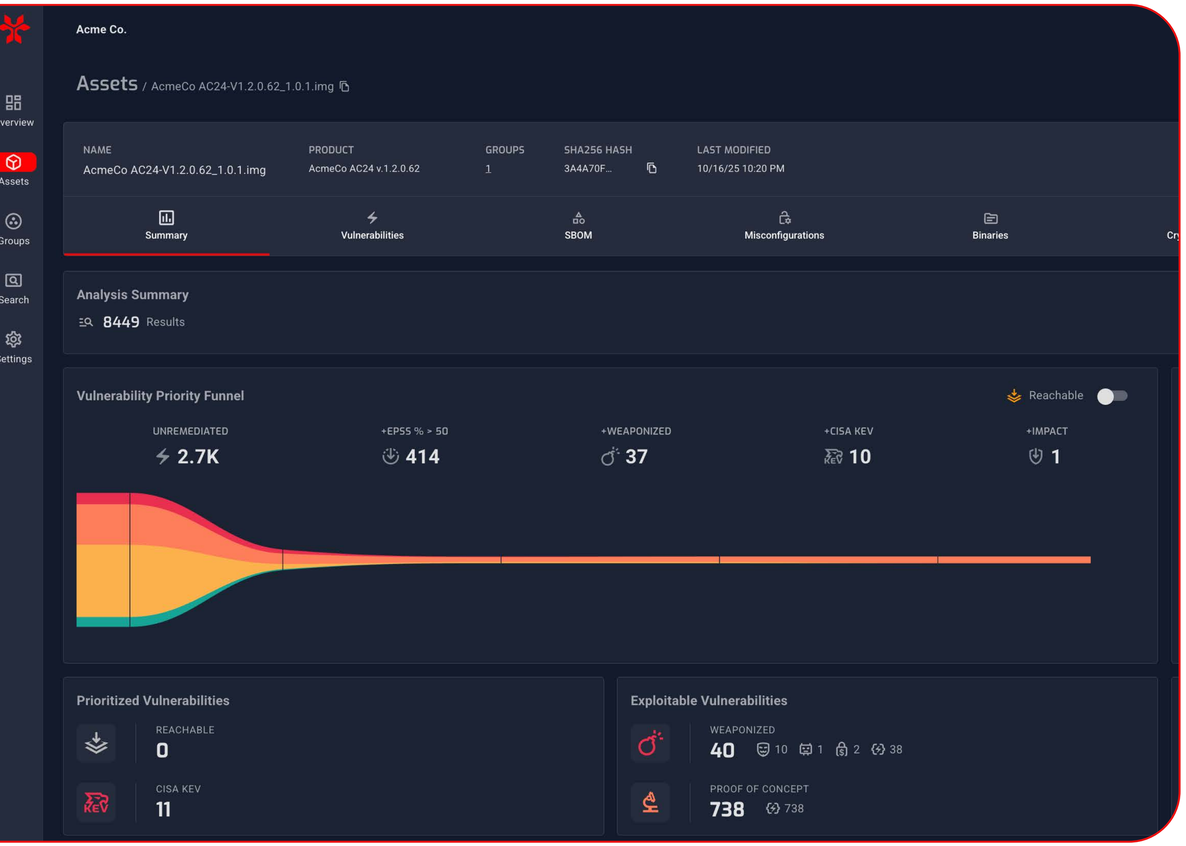
For most agencies, the first practical step in a PQC program is not deploying new algorithms. It is establishing a comprehensive inventory of cryptographic assets and dependencies.

Venables makes this point directly: agencies must first identify where cryptography that needs to be updated actually resides, including in libraries, embedded software, hardware, and supply chains. This is where many organizations run into trouble. Traditional asset and software inventory approaches often stop at the application layer or depend on what vendors disclose. That leaves blind spots.

In federal environments, those blind spots matter:

- mission systems may rely on legacy or unsupported components
- fielded devices may contain embedded cryptography that is not visible through conventional tooling
- third-party and supplier-provided systems may introduce inherited risk
- software signing and authentication paths may be more mission-critical than data confidentiality alone

Agencies cannot prioritize what they cannot see.




# Why deep software visibility is critical to a federal PQC strategy

This is where NetRise's data becomes operationally important.

NetRise helps agencies create a comprehensive software asset inventory that identifies cryptographic assets at the binary level, including in firmware, compiled software, and third-party components. That matters because PQC planning requires visibility beyond what source code repositories, manifests, or application-layer scans can provide.

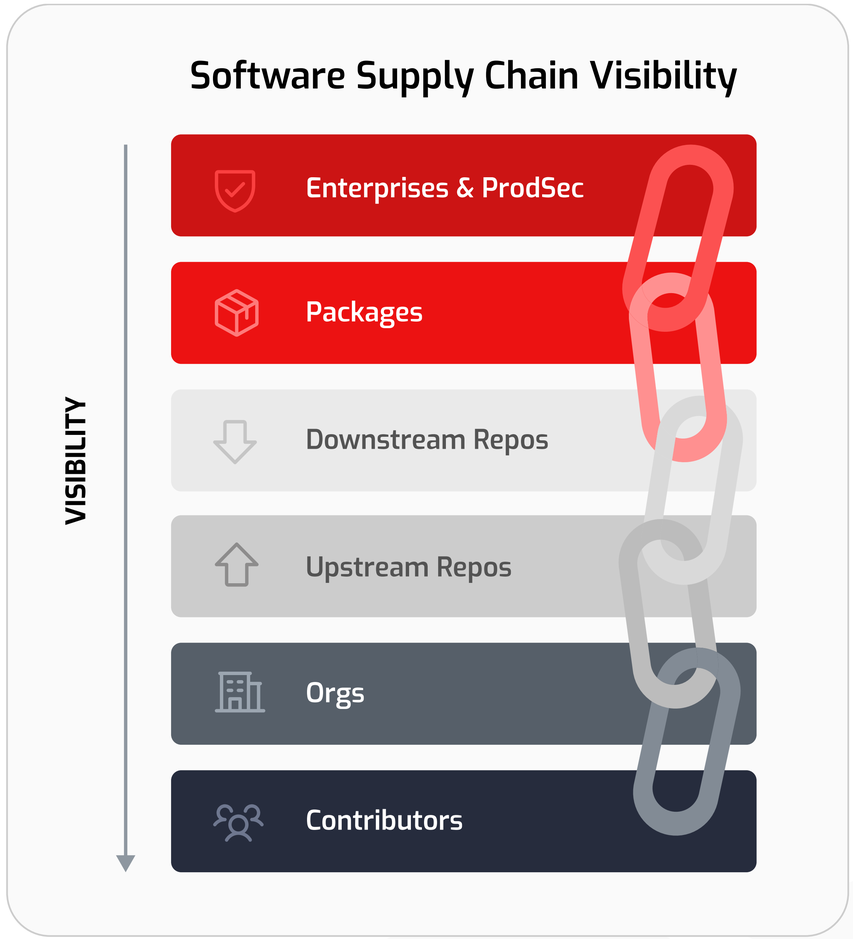
From a federal guidance standpoint, there are four reasons this kind of data is essential.

1

# It provides the comprehensive inventory agencies need

A credible PQC migration plan starts with knowing where classical cryptography exists across the enterprise. In most agencies, the answer will span far beyond business applications. It will include embedded systems, appliances, operational technology, fielded assets, and vendor-supplied software. Venables explicitly advises organizations to scope broadly, including hardware and the extended enterprise.

Binary composition analysis helps agencies do exactly that.



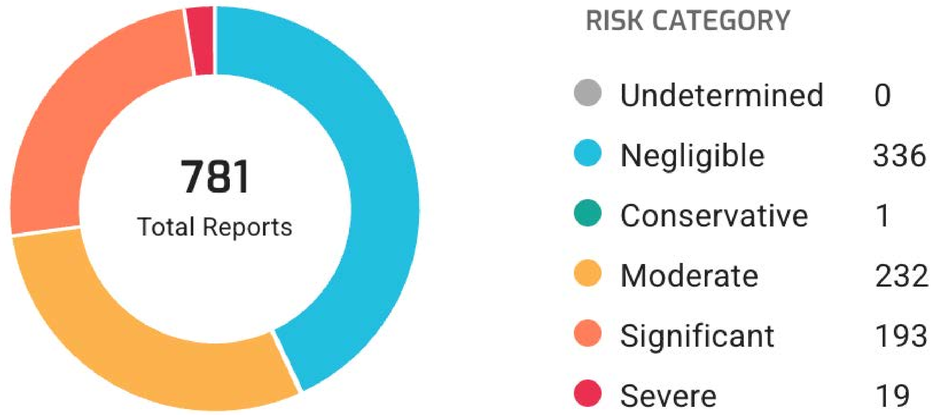
# 2

## It enables risk-based prioritization

Most findings today will point to classical cryptographic algorithms. That is not surprising. The important question is not whether agencies find classical cryptography. They will. The important question is where it matters most.

Agencies need to identify:

- systems supporting authentication and trust chains
- software signing infrastructure
- systems protecting sensitive but long-lived data
- operationally critical devices with long field lifetimes
- supplier-provided technologies that may lag in PQC readiness



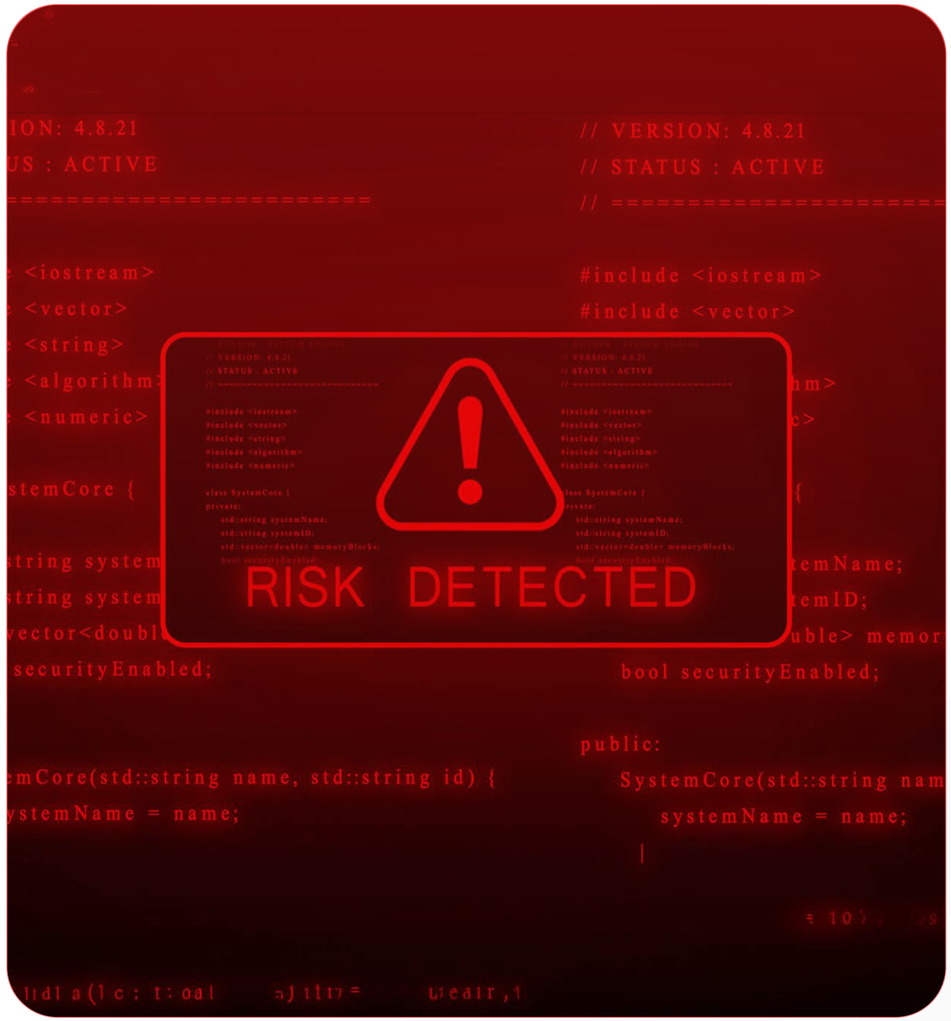

**Google's research underscores that viable PQC solutions exist, but they will take time to implement. That means prioritization is not optional. It is the heart of the strategy.**

# 3

# It reduces supply chain and embedded system blind spots

Federal agencies rarely operate in clean, fully transparent environments. Much of the risk sits in third-party code, compiled packages, firmware, and inherited technology stacks. Traditional discovery methods often miss those layers. NetRise addresses the visibility problem by analyzing the software artifact itself, rather than relying solely on declarations about it.

That is especially important for agencies managing critical infrastructure, defense systems, civilian operational technology, or large distributed environments where embedded cryptography may remain in service for years.



# 4

## It supports long-term crypto agility

PQC is not a single swap-out event. Venables stresses the importance of crypto agility, including the possibility that parameters, key sizes, or algorithms may need to change over time. Agencies therefore need durable visibility, not just a one-time inventory exercise.

A living cryptographic inventory supports:

- transition planning
- validation of remediation progress
- policy enforcement for new procurement
- response to future standards changes or implementation risks

# Recommended guidance for federal agencies

Based on the current research and migration guidance, agencies should consider the following approach:

### Start with comprehensive cryptographic discovery.

Inventory cryptographic implementations across software, firmware, hardware, and third-party components, not just known application stacks.

### Treat binary-level visibility as foundational.

Do not assume manifests, bills of materials, or vendor attestations are enough to expose embedded or inherited cryptographic dependencies.

### Prioritize by mission impact.

Focus first on systems involved in authentication, software signing, sensitive long-lived data, and assets with long replacement cycles. Venables notes that signing and authentication keys may be among the most critical to address.

### Plan for hybrid and phased operation.

Agencies should expect coexistence between current and post-quantum cryptographic approaches for the foreseeable future.

### Extend requirements into procurement and suppliers.

PQC readiness is not just an internal engineering matter. It must influence acquisition, vendor roadmaps, and supply chain assurance.

# Federal POV

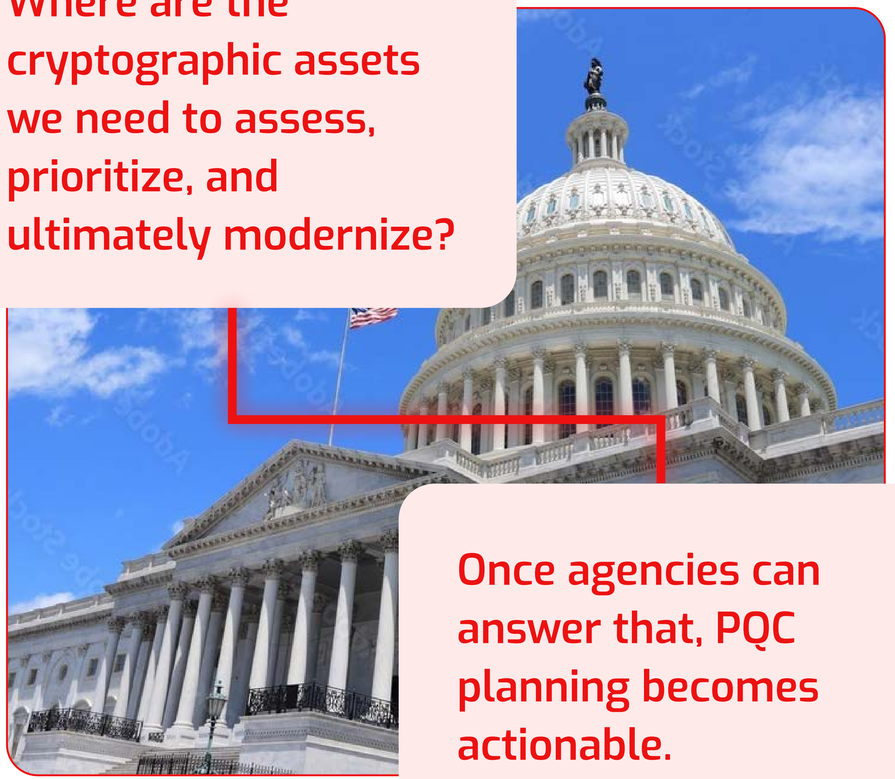
For federal agencies, the PQC challenge is no longer theoretical and it is not primarily a standards problem. It is a visibility and execution problem.

Agencies do not need to wait for every migration decision to be finalized before acting. They can act now by building the one thing every successful PQC strategy requires: a comprehensive, defensible understanding of where cryptography exists across their environment.

That is why NetRise data is so important to a federal PQC strategy.

NetRise helps agencies answer the first, hardest, and most operationally important question in post-quantum planning.

**Where are the cryptographic assets we need to assess, prioritize, and ultimately modernize?**



**Once agencies can answer that, PQC planning becomes actionable.**

NETRISE

# What's Inside *Your* Software?

Talk with our experts