Lumen Next Generation Network Cryptography Program

A Quantum-Resilient Blueprint for Government Agencies

Government agencies are under increasing pressure to modernize cryptography while keeping mission-critical operations running without disruption. As quantum computing, AI-driven threats, and data-harvesting tactics accelerate, leaders must address cryptographic risk across complex, distributed environments, often without clear visibility into how encryption is implemented or where operational constraints exist.

In many environments, agencies rely on a mix of cryptographic approaches, some optimized for high assurance, others for agility and scale. Understanding where existing cryptographic controls support mission needs and where they introduce friction, risk, or future constraints is a prerequisite to effective modernization. Lumen Next Generation Network Cryptography (NGNC) begins with an automated, AI-driven discovery and planning capability that provides this clarity, defining what needs to be addressed, in what order, and with minimal operational risk.

Lumen Next Generation Network Cryptography (NGNC)

Lumen Next Generation Network Cryptography is an end-to-end program designed to help public sector agencies assess, modernize, and sustain quantum-resilient network security without disrupting operations.

> "Your data is being stolen today to be decrypted tomorrow. Modern encryption is not a safeguard, it's a countdown"
>
> — **Tom Barnett,** Director of Strategic Innovation, Lumen

NGNC begins with Discovery, Inventory, and Planning: an automated, AI-driven investigative phase that identifies cryptographic assets across networks, systems, applications, code, and encrypted traffic. This step evaluates classical and post-quantum risk and produces a prioritized remediation and migration roadmap.

Challenges redefining encryption standards

Limited cryptographic visibility: Agencies often lack a complete, up-to-date understanding of where cryptography is used across networks, applications, code, and encrypted traffic—making risk difficult to assess and prioritize.

Data harvesting risk: "Harvest now, decrypt later" tactics expose long-lived data to future compromise, increasing the need for forward-looking cryptographic planning.

AI-accelerated threats: AI-enabled tools are increasing the speed and scale of cryptographic exploitation, placing additional pressure on already complex environments.

Post-quantum transition pressure: Preparing for post-quantum cryptography requires more than algorithm replacement—it demands careful planning to avoid disruption across mission-critical systems.

LUMEN® TECHNOLOGIES

As a certified NSA Trusted Integrator, Lumen applies these findings to design and implement accredited cryptographic architectures including CSfC-aligned and post-quantum-ready solutions ensuring NGNC deployments meet assurance requirements while remaining scalable, adaptable, and operationally viable.

NGNC Framework

The NGNC Framework allows agencies to adopt one or more cryptographic capabilities independently, based on mission needs, risk priorities, and budget. Capabilities are not bundled or mandatory and may be implemented individually or phased over time to align with operational requirements.

Each capability is designed to integrate with existing environments and approved security architectures, enabling agencies to modernize cryptography with minimal, if any, disruption to mission-critical operations. This lifecycle is supported by Lumen Black Lotus Labs, which validates emerging cryptography and AI-enabled threat techniques and prototypes future network architectures, helping keep the network (and in-turn agency operations) secure as threats evolve.

Discovery, Inventory, and Planning (Foundational Phase)

Each NGNC capability includes built-in discovery and assessment functions appropriate to its scope, helping identify relevant cryptographic dependencies and risks as part of implementation.

For agencies that require comprehensive visibility, NGNC also offers an optional Discovery, Inventory, and Planning capability. This standalone service provides deeper analysis across networks, hosts, applications, containers, code repositories, and encrypted interfaces. It identifies cryptographic assets, evaluates classical and post-quantum risk, and produces a prioritized remediation and migration roadmap.

Agencies may engage the Discovery, Inventory, and Planning capability independently or rely on the embedded discovery within individual NGNC capabilities, depending on mission objectives, risk tolerance, and available resources.

Quantum Multi-Encryption Framework (QMEF)

Enables classified assurance using dual-layer commercial encryption, replacing rigid legacy systems like TACLANEs with agile, scalable alternatives. This approach minimizes complexity while helping maintain NSA compliance and accelerates deployment timelines.

Quantum Mobility Protocol-Free Encryption Device (PFED)

A protocol-agnostic, AI-autonomous encryptor that secures digital payload voice, video, ATM frames, serial, IPv6 without requiring protocol translation. It supports VLAN segmentation, galvanic isolation, and ephemeral keying for resilient security in disconnected environments through autonomous key management and post-quantum algorithms.

Post-Quantum Encryption (PQE)

Uses CRYSTALS-Kyber and other NIST- and NSA-aligned algorithms to resist quantum decryption helps ensure harvested data remains secure against future quantum threats.

Quantum Key Distribution (QKD): Helps ensure secure key exchange using quantum mechanics, mitigating risks of interception and replay attacks. QKD is a foundational element in building a truly quantum-resilient infrastructure.

Lumen Private Connectivity Fabric (LPCF)

Integrates these capabilities into a unified, scalable platform that enables secure mobility and interoperability across mission domains. From a network infrastructure perspective, LPCF can serve as the connectivity foundation supporting secure interconnect, segmentation, and policy consistency across multi-site and hybrid environments. It helps resolve fragmented infrastructure by supporting dynamic scalability, consistent policy enforcement, and AI-driven workloads with an approach designed to preserve performance and align with applicable compliance requirements.

866-352-0291 I lumen.com I info@lumen.com

LUMEN® TECHNOLOGIES

Together, these NGNC capabilities form a flexible, mission-ready architecture designed to support evolving cryptographic requirements while supporting operational continuity during transition. Informed by discovery-led planning, NGNC enables agencies to address current threats, prepare for post-quantum transitions, and adapt securely as mission needs change.

How can agencies benefit?

NGNC is designed to help government agencies experience:

- Clear visibility into cryptographic risk across networks, applications, and encrypted traffic
- Reduced modernization risk through prioritized, data-driven remediation planning
- Operational continuity during change, helping minimize disruption to mission-critical services
- Fast, accurate NGNC deployments informed by validated discovery findings
- Audit-ready documentation supporting OMB, CISA, and NSA cryptographic inventory requirements
- Simplified operations through managed services and automation, allowing teams to focus on mission outcomes

NGNC is more than a collection of cryptographic technologies, it is a strategic approach to delivering secure, scalable, and sovereign communications across complex government environments.

Future-Ready your agency

If you're a CISO, CIO, or IT leader, contact Lumen today to:

- Schedule a cryptographic discovery and NGNC readiness briefing
- Understand where cryptographic risk exists across your environment
- Explore NGNC deployment options aligned to your mission and assurance requirements

Start with discovery. Modernize with confidence.

- Contact Lumen to schedule a cryptographic discovery and NGNC readiness briefing designed to help your agency understand current risk, prioritize remediation, and accelerate the transition to quantum resilient network security without disrupting operations.

Why Lumen?

Lumen is positioned to guide agencies through quantum-era modernization because we address the full lifecycle from discovery through deployment and operations.

Unlike providers that begin with encryption products, Lumen starts by defining the problem. Our AI-driven cryptographic discovery and planning capability provides agencies with a prioritized view of remediation needs, helping reduce uncertainty, support operations, and guide NGNC deployments.

866-352-0291 I lumen.com I info@lumen.com

LUMEN® TECHNOLOGIES