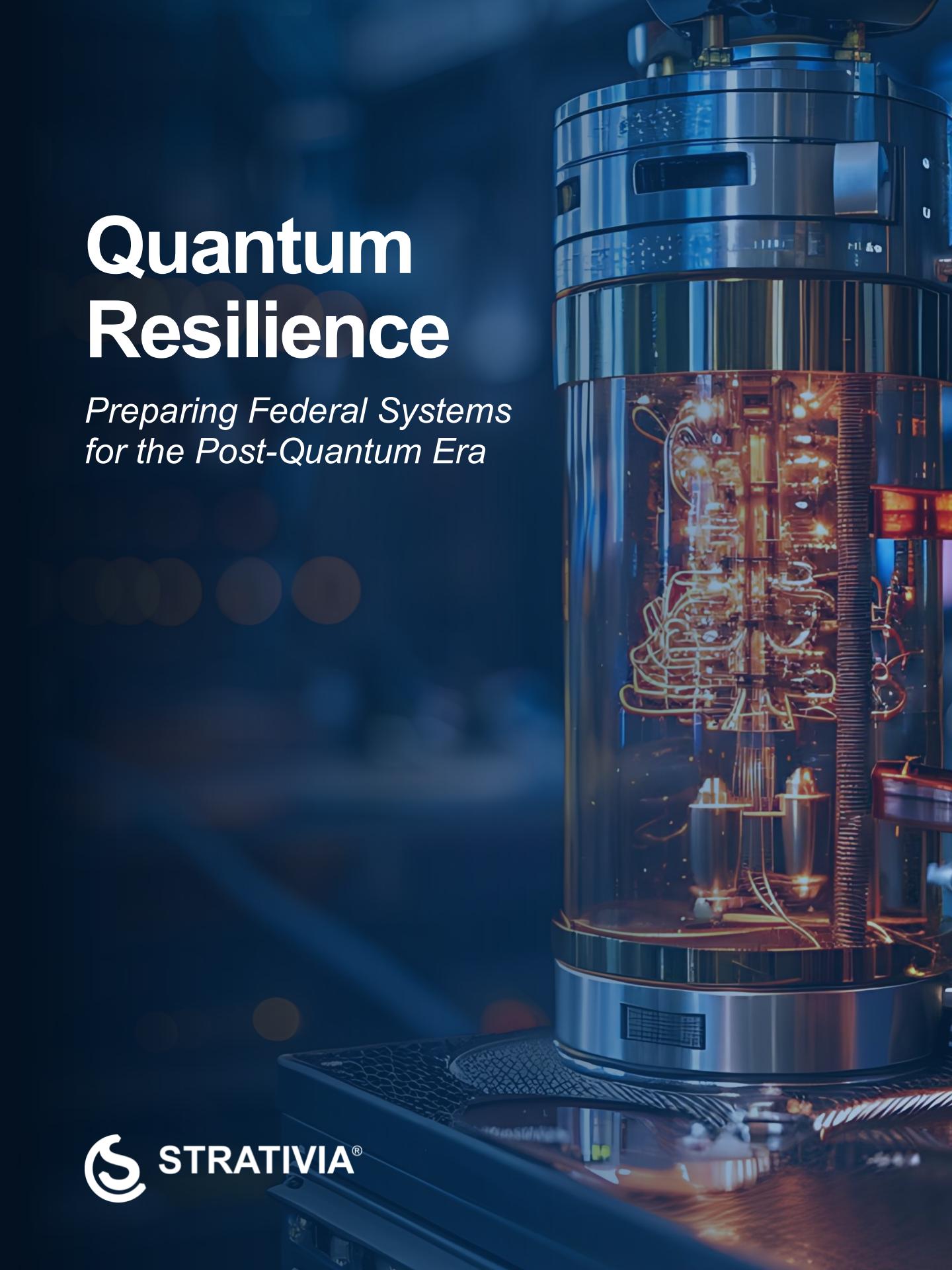
Quantum Resilience

Preparing Federal Systems for the Post-Quantum Era



STRATIVIA®

Quantum Resilience

Preparing Federal Systems for the Post-Quantum era

Introduction

Strativia understands that quantum computing is no longer a distant scientific concept—it is a near-term technological reality with enormous implications for national security, encryption standards, and digital infrastructure. As the U.S. government accelerates its quantum readiness initiatives, the need to understand, assess, and act on post-quantum risks has never been more critical.

With experience supporting mission-critical systems for agencies like DOE and NIST, Strativia helps federal leaders navigate the emerging challenges posed by quantum disruption—bringing deep understanding of both legacy system architecture and the next-generation technologies that will transform it.

Understanding the Quantum Threat

Quantum computers promise unprecedented computational power. But with that power comes a paradox: many of the cryptographic algorithms that underpin today's secure communications—RSA, ECC, and others—will be rendered obsolete by sufficiently capable quantum machines.

This 'Q-Day' risk has spurred action across the federal space. The National Institute of Standards and Technology (NIST) has already selected quantum-safe algorithms, and the White House has issued a National Security Memorandum (NSM-10) mandating quantum-resilient cryptographic transition planning for all federal agencies.

Strategic Imperatives for Federal Agencies

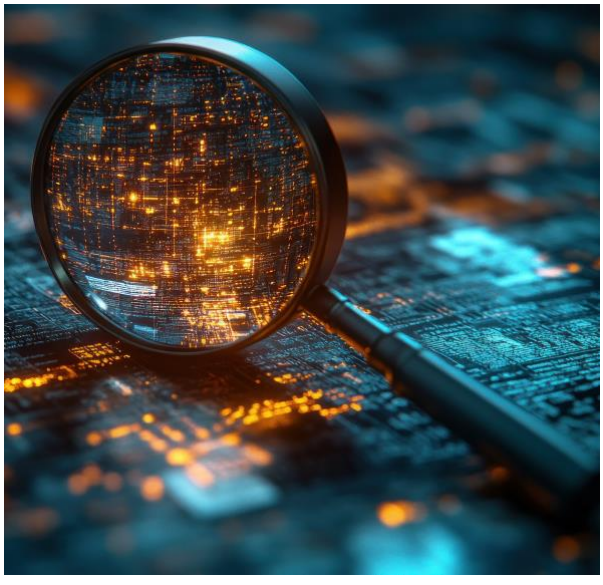
Becoming quantum-resilient isn't just a technology upgrade—it requires strategic planning, risk assessment, and enterprise-wide coordination. Agencies must:

- Inventory and assess cryptographic assets and protocols
- Align with NIST's post-quantum cryptography (PQC) standards
- Develop migration roadmaps with key partners and vendors
- Integrate quantum considerations into cybersecurity, AI, and data architecture strategies

From Communication to Countermeasures

Strativia brings a mission-first approach to quantum transformation. Our services are built for operational relevance, policy alignment, and technical flexibility.
We support agencies in the following areas:

- Post-quantum risk assessments and system inventories
- PQC-aligned configuration and transition planning
- Zero Trust architectures adapted for quantum resilience
- Staff augmentation and cleared technical personnel for classified or emerging tech programs



Case Snapshot: Enabling Quantum Planning at DOE Transition

Strativia supported a multi-year information assurance engagement with the Department of Energy that included early assessments of cryptographic dependency and risk exposure in legacy applications. We helped establish the foundation for future post-quantum migration, aligning agency practices with both internal directives and external NIST guidance.

The Strativia Commitment: Technology that Secures the Mission

At Strativia, we combine the rigor of a prime contractor with the responsiveness of an innovation partner. As a CMMI Level 3, ISO 27001–certified firm with Top Secret–cleared personnel, we help agencies embrace next-gen technologies like quantum computing while preserving compliance, operational integrity, and public trust.

Let's secure the future—together.

Strativia (HQ)
1401 Mercantile Lane, Suite 501, Largo, MD 20774
P: 301-362-6555 | F: 301-362-6557 | www.strativia.com

Strativia Regional Offices:
Arlington, VA | Atlanta, GA | Denver, CO

STRATIVIA®
TECHNOLOGY | CONSULTING | SERVICES