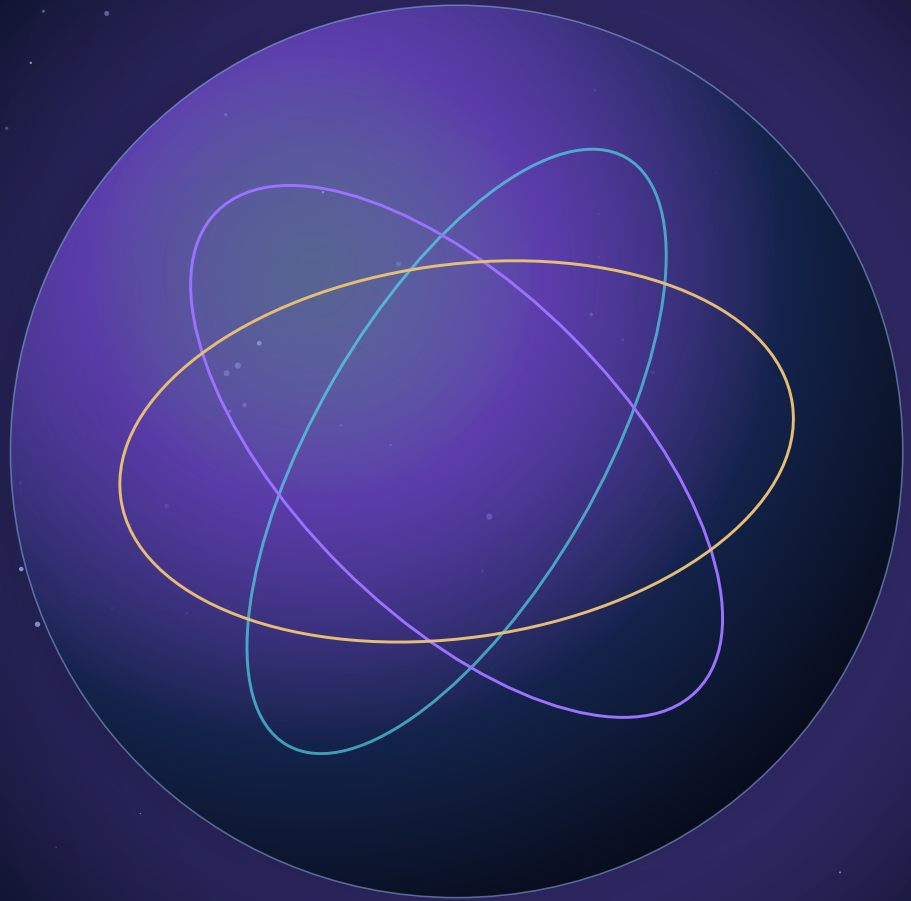




◆ OBSERVATORY ANALYSIS

The Post-Quantum Migration Guidance Is Final

How a quantum computer that does not yet exist is already
reorganizing the security of the world economy

PUBLICATION RECORD

IDENTIFIER	QCO-2026-006
SERIES	Quantum Civilization Observatory Analyses
TITLE	The Post-Quantum Migration Guidance Is Final: How a quantum computer that does not yet exist is already reorganizing the security of the world economy
TYPE	Observatory analysis
VERSION	1.1 · published 28 October 2026
AUTHOR	Steven Alber
INSTITUTION	Quantum Civilization
PUBLISHER	Quantum Civilization
HISTORY	1.1 · 28 October 2026 · Author attribution added: Steven Alber (author), Quantum Civilization (institution and publisher). 1.0 · 28 October 2026 · First edition.
CITE AS	Alber, S. (2026). The Post-Quantum Migration Guidance Is Final. Quantum Civilization Observatory Analyses, QCO-2026-006, version 1.1. Quantum Civilization. https://quantumcivilization.org/observatory/nist-pqc-transition/
ONLINE	https://quantumcivilization.org/observatory/nist-pqc-transition/

Abstract

NIST finalized its guidance for moving away from quantum-vulnerable public-key cryptography: institutions are reorganizing on the schedule of an anticipated machine. Development: 27 October 2026 · NIST · IR 8547 · Official technical report.

KEYWORDS Quantum Observatory · policy · L5

The Post-Quantum Migration Guidance Is Final

The result

On 27 October 2026 the U.S. National Institute of Standards and Technology finalized IR 8547, its guidance for the transition from quantum-vulnerable public-key cryptography to post-quantum standards [1]. The final report replaces the initial public draft released in November 2024 [2]. It builds on the three post-quantum standards NIST approved in August 2024: FIPS 203, 204 and 205 [3].

What it establishes

Public-key algorithms such as RSA and elliptic-curve cryptography protect most of the world's digital communication and could be broken by a sufficiently large fault-tolerant quantum computer running Shor's algorithm. No such machine exists. The migration is driven by expectation: data encrypted today can be recorded and decrypted later, and replacing cryptography across governments, banks, devices and software supply chains takes many years. The final report converts that expectation into a formal transition path for one of the world's most influential standards bodies.

Position in the Civilizational Compute Stack

L5, institutions, reached without passing through the lower layers. That is what makes this development analytically unusual.

Why it matters

Quantum computing is the first technology whose institutional consequences arrive on a schedule set by its anticipated future rather than its present performance. Billions in migration spending, procurement rules and compliance regimes are being set in motion by a capability forecast. The same pattern can be expected in export controls, national investment and research security, which is why tracking the gap between anticipated and demonstrated capability is a central task of Quantum Civilization.

The open question

How fast does the installed base actually migrate, and which sectors and countries fall behind the timeline?

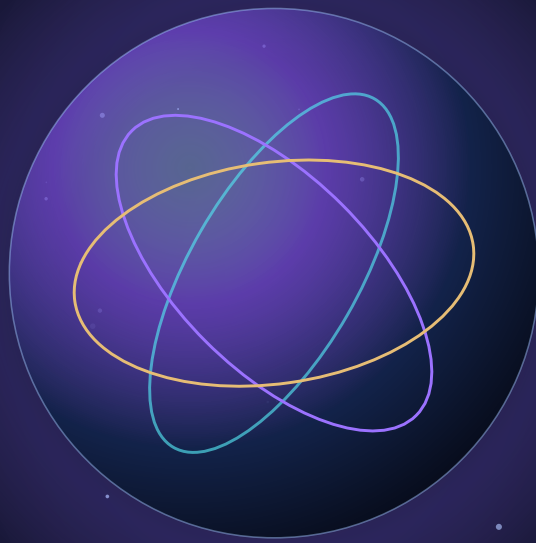
Signposts

Sectoral migration deadlines adopted by regulators; post-quantum algorithms enabled by default in major protocols and platforms; national guidance outside the United States aligning with or diverging from NIST.

REFERENCES

Sources

- 1 NIST. IR 8547: Transition to Post-Quantum Cryptography Standards (final). 27 October 2026.
OFFICIAL TECHNICAL REPORT
<https://csrc.nist.gov/pubs/ir/8547/final>
- 2 NIST CSRC. IR 8547 initial public draft (November 2024), obsoleted on 27 October 2026 by the final report.
OFFICIAL RECORD
<https://csrc.nist.gov/pubs/ir/8547/ipd>
- 3 NIST. Announcing approval of three Federal Information Processing Standards for post-quantum cryptography. 13 August 2024.
OFFICIAL STANDARDS ANNOUNCEMENT
<https://www.nist.gov/news-events/news/2024/08/announcing-approval-three-federal-information-processing-standards-fips>



QUANTUM
CIVILIZATION
RESEARCH INSTITUTE

Physics will decide what becomes computable.
Institutions will decide what becomes of it.