Tanaq
INTEGRATED TECHNOLOGIES DIVISION

WHITE PAPER

Post Quantum Cryptography Comprehensive Publication Research Index

A curated index of 355 sources across 26 subject areas, tracking the research, standards, legislative, and policy developments that define the Federal post quantum landscape.

Roger Payne, President, Tanaq Integrated Technologies

Created: August 13, 2025 | Updated: July 21, 2026

ABOUT THIS INDEX

Why we maintain this

This edition adds 47 new sources across nine new sections covering the research, standards, legislative, and policy developments that now define the post quantum landscape: the June 2026 executive orders and OMB Memorandum M-26-15, congressional quantum legislation, the Department of War Post Quantum Cryptography Strategy, NIST standards status, CISA and NSA procurement guidance, IETF protocol integration, quantum algorithm and cryptanalysis research, hardware milestones, industry deployment, and international financial sector coordination, while outdated and superseded sources have been removed to keep the index current. A Federal PQC compliance timeline follows for quick reference.

The post quantum transition is not a single procurement decision. It is a multi year migration governed by executive order, OMB memoranda, NIST standards, and agency specific guidance that continues to move. Agencies that inventory their cryptography early migrate on their own terms. Agencies that wait migrate on a deadline.

Tanaq Integrated Technologies maintains this index so that program managers, security officers, and contracting officers have one current, sourced reference rather than a scatter of vendor marketing. Entries are annotated so a reader can judge relevance before following a link, and superseded sources are removed rather than left to age.

HOW TO USE IT

The compliance timeline that follows is the quick reference. The sections that follow move from foundational concepts through the threat, the standards, the Federal mandate, and the current state of industry deployment. Each entry carries its source and a short annotation of what it establishes.

QUICK REFERENCE

Federal PQC Compliance Timeline

Date	Milestone
August 13, 2024	NIST publishes FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) as final standards.

Date	Milestone
December 2024	NSA revises CNSA 2.0 to version 2.1 for National Security Systems; Google demonstrates below threshold quantum error correction on the Willow processor.
March 11, 2025	NIST selects HQC as the fifth PQC algorithm; NIST IR 8545 documents the decision.
May 21, 2025	Gidney (Google Quantum AI) cuts the RSA-2048 factoring estimate to under one million noisy qubits.
June 6, 2025	Executive Order 14306 preserves the PQC mandates of EO 14144 and directs the CISA product list and TLS 1.3 adoption by January 2, 2030.
January 2026	CISA and NSA publish the PQC product categories list; the G7 Cyber Expert Group issues its financial sector PQC roadmap.
April 2026	Senate and House committees advance the National Quantum Initiative Reauthorization Act (S.3597 and H.R. 8462), extending the initiative through 2034 with new PQC provisions.
June 22, 2026	President signs Executive Order 14412 (PQC migration) and Executive Order 14413 (quantum innovation).
June 23 to 24, 2026	The Department of War releases its Post Quantum Cryptography Strategy; OMB issues M-26-15 with a five phase schedule through 2035.
December 31, 2030	EO 14412: PQC key establishment on high value assets and high impact systems; Federal contractors comply with PQC FIPS; all DoW systems support PQC or phase out; NIST deprecates 112 bit classical public key algorithms after 2030.
December 31, 2031	EO 14412: PQC digital signatures in place; all DoW systems use PQC.

Date	Milestone
2035	Full Federal migration complete per M-26-15 and NSM-10; NIST disallows quantum vulnerable public key algorithms.

CONTENTS

Sections

01	**Federal PQC Compliance Timeline**	
02	**Foundational Concepts: What is Quantum Computing?**	3 sources
03	**The Quantum Threat to Cybersecurity**	7 sources
04	**Key Quantum Algorithms: Shor's and Grover's**	9 sources
05	**The Solution: Post Quantum Cryptography (PQC)**	9 sources
06	**Timelines and Standardization Efforts**	21 sources
07	**Industry Use Cases and Impact**	11 sources
08	**National Security and Government**	3 sources
09	**Market Trends and Future Outlook**	24 sources
10	**PQC Standards and Implementation**	14 sources
11	**Business Risks and Impacts**	8 sources
12	**Industry Solutions and Readiness**	17 sources
13	**Market and Vendor Landscape**	7 sources
14	**Technical Implementation and Analysis**	9 sources
15	**Government and Policy**	133 sources
16	**Crypto Agility**	9 sources
17	**Historical Transitions and Military Applications**	24 sources

18	**The June 2026 Federal Mandate: Executive Orders, OMB M-26-15, and the DoW Strategy**	13 sources
19	**Congressional Action and Pending Legislation**	7 sources
20	**NIST Standards and Guidance Updates**	5 sources
21	**CISA and NSA Procurement Guidance**	3 sources
22	**Protocol Standards and Internet Integration**	2 sources
23	**Quantum Algorithms and Cryptanalysis Research**	3 sources
24	**Quantum Threat Research and Hardware Milestones**	6 sources
25	**Industry Deployment and Market Acceleration**	6 sources
26	**International and Financial Sector Coordination**	2 sources

SECTION 01

Federal PQC Compliance Timeline

SECTION 02

Foundational Concepts: What is Quantum Computing?

1. What Is Quantum Computing? | IBM

https://www.ibm.com/think/topics/quantum-computing

Quantum computing leverages quantum mechanics to solve problems too complex for classical computers. This creates immense opportunities but also presents a fundamental threat to current cybersecurity.

2. Quantum Computing vs. Classical Computing - Black Box

http://www.blackbox.com/insights/blogs/detail/tps/2024/03/12/more-than-a-bit-about-quantum-qubit-computing

Unlike classical computers using bits (0s and 1s), quantum computers use qubits that can be both 0 and 1 simultaneously, enabling exponential processing power. This capability is the reason they can break current encryption standards that are safe from classical attacks.

3. What is quantum computing and how does it work? - Iberdrola

https://www.iberdrola.com/innovation/what-is-quantum-computing

This article explains that quantum computing uses principles like superposition and entanglement to achieve massive parallel processing power. Businesses should understand this technology as it will disrupt industries by solving complex optimization, material science, and pharmaceutical problems.

SECTION 03

The Quantum Threat to Cybersecurity

4. Quantum computing RSA encryption: a threat and a solution -Freemindtronic

https://freemindtronic.com/quantum-computing-rsa-encryption-freemindtronic-nfc-technology/

Quantum computers pose a direct threat to RSA encryption, a cornerstone of today's digital security. This article frames the urgent business need to transition to quantum resistant solutions to protect sensitive data and digital transactions.

5. The Invisible Threat: How Quantum Computing Could Break Today's Encryption? | by Akitra

https://medium.com/@akitrablog/the-invisible-threat-how-quantum-computing-could-break-todays-encryption-888e3ea99cf3

The primary business risk from quantum computing is its ability to break the public key encryption that protects virtually all digital communications and data. This makes the transition to new security standards a critical priority for risk management and business continuity.

6. Quantum-Safe Cryptography: Hype versus Reality - ipSpace.net blog

https://blog.ipspace.net/kb/QuantumCrypto/

This article cuts through the hype to confirm that the quantum threat to current encryption is real and requires a transition to new algorithms. For executives, it clarifies that while timelines are debated, the need for a migration strategy is not.

7. Quantum Computing - How it Changes Encryption as We Know It

https://it.umd.edu/security-privacy-audit-risk-and-compliance-services-sparcs/topic-week/quantum-computing-how-it-changes-encryption-we-know-it

Quantum computing will fundamentally reset the landscape of digital encryption, rendering current standards obsolete. Businesses must prepare for a comprehensive overhaul of their security infrastructure to protect against this paradigm shift.

8. How to stop quantum computers from breaking the internet's encryption - Science News

https://www.sciencenews.org/article/quantum-computers-break-internet-save

The global technology community is in a race to develop and deploy new, quantum resistant algorithms to prevent a catastrophic failure of internet security. This highlights the critical importance of the ongoing NIST standardization process for business and national security.

9. Quantum vs Classical Computing | Quantum Threat | Quantropi

https://www.quantropi.com/quantum-versus-classical-computing-and-the-quantum-threat/

This source contrasts classical and quantum computing to explain precisely why the latter poses a unique threat to modern cryptography. Understanding this difference is key to justifying investments in next -generation, quantum safe security solutions.

10. Quantum Computing vs. Classical Computing: What's the Difference? - BlueQubit

https://www.bluequbit.io/quantum-computing-vs-classical-computing

By explaining the core differences in how quantum and classical computers process information, this article clarifies why quantum systems can solve problems, like breaking encryption, that are impossible for current machines. This technical reality drives the need for a strategic shift in cybersecurity.

SECTION 04

Key Quantum Algorithms: Shor's and Grover's

11. Shor's Algorithm: How Quantum Computers Might Break Cryptography - Soumyadip Sarkar

https://neuralsorcerer.medium.com/shors-algorithm-how-quantum-computers-might-break-cryptography-95f25b16cd51

Shor's algorithm is the specific quantum formula that directly targets the mathematical underpinnings of RSA and ECC, the most common forms of public key encryption. Its proven effectiveness is the primary technical reason that migration to new cryptographic standards is necessary.

12. What is Shor's Algorithm - QuEra

https://www.quera.com/glossary/shors-algorithm

This glossary entry provides a concise definition of Shor's algorithm as the tool that enables quantum computers to factor large numbers efficiently. Its existence makes the obsolescence of current public key infrastructure a certainty, creating a clear mandate for businesses to upgrade their systems.

13. Shor's Algorithm - Classiq

https://www.classiq.io/insights/shors-algorithm

This article explains the mechanics of Shor's algorithm, the quantum process that will break the encryption protecting most of the world's secure data. Understanding this specific threat allows leaders to frame the PQC transition as a direct countermeasure to a known vulnerability.

14. Can Quantum computers break RSA encryption? | by Nour Oulad Moussa - Medium

https://medium.com/@nour.oulad.moussa/can-quantum-computers-break-rsa-encryption-cf281204c21d

The answer is an unequivocal yes, thanks to Shor's algorithm, which makes factoring large numbers, the basis of RSA's security, trivial for a capable quantum computer. This fact eliminates any debate about the need for a transition to quantum resistant encryption.

15. What is Shor's Algorithm? - Utimaco

https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-shors-algorithm

This piece positions Shor's algorithm as the primary catalyst for the global migration to post quantum cryptography. For executives, it clarifies that the threat isn't abstract but is based on a specific, known quantum algorithm that renders current security models obsolete.

16. Shor's algorithm

https://www.qutube.nl/quantum-algorithms/shors-algorithm

This resource explains the principles behind Shor's algorithm, providing a clear technical basis for the quantum threat to modern encryption. It reinforces the business imperative to move away from cryptographic systems vulnerable to this specific attack.

17. What is Grover's Algorithm? - YouTube

https://www.youtube.com/watch?v=_cDIzwycANg

This video explains Grover's algorithm, a quantum search method that weakens symmetric encryption like AES but does not completely break it. The primary business takeaway is that while AES remains viable with larger key sizes, asymmetric encryption requires a complete replacement.

18. Theory of Grover Search Algorithm - Azure Quantum | Microsoft Learn

https://learn.microsoft.com/en-us/azure/quantum/concepts-grovers

This document details the theory behind Grover's algorithm, which makes searching large databases significantly faster with a quantum computer. For security, this means symmetric keys (like AES) are less secure, necessitating a transition to longer keys (e.g., AES-256) as part of a comprehensive quantum readiness plan.

19. What is Grover's Algorithm? - Utimaco

https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-grovers-algorithm

Grover's algorithm reduces the security of symmetric encryption standards like AES by effectively halving their key strength. This requires businesses to migrate from AES-128 to AES-256 to maintain a sufficient security margin in the quantum era.

SECTION 05

The Solution: Post Quantum Cryptography (PQC)

20. Quantum-safe Cryptography Algorithms - IBM Research

https://research.ibm.com/projects/quantum-safe-cryptography

IBM Research is actively developing and contributing to new cryptographic algorithms designed to be secure from quantum computer attacks. This demonstrates significant industry investment in creating viable solutions for the PQC transition, providing businesses with confidence in the forthcoming standards.

21. Post-quantum cryptography

https://openquantumsafe.org/post-quantum-crypto.html

The Open Quantum Safe project is a collaborative open -source effort to develop and standardize quantum -resistant cryptography. This initiative is crucial for providing businesses with accessible, well vetted tools to implement PQC and accelerate the globa l transition.

22. Breaking RSA with a Quantum Computer - Schneier on Security

https://www.schneier.com/blog/archives/2023/01/breaking-rsa-with-a-quantum-computer.html

Renowned security expert Bruce Schneier analyzes the practical requirements for breaking RSA with a quantum computer, confirming the threat is real but dependent on hardware maturity. For executives, this reinforces that while the "Q-Day" is not here yet, the "harvest now, decrypt later" threat makes immediate preparation essential.

23. The Rise of Quantum-Resistant Cryptography - IEEE Computer Society

https://www.computer.org/publications/tech-news/trends/quantum-resistant-cryptography/

This article chronicles the development of quantum resistant cryptography as a direct response to the threat posed by quantum computers. It frames PQC not as a niche issue but as the next major evolution in cybersecurity that all businesses must prepare for.

24. Quantum Computing and the Future of Encryption - Scholarly Review Journal

https://www.scholarlyreview.org/article/127168.pdf

This academic paper provides a formal analysis of the impact of quantum computing on encryption, solidifying the business case for migrating to PQC. It serves as a foundational document for understanding the long term strategic implications of the quantum threat.

25. Breaking 256-bit Elliptic Curve Encryption with a Quantum Computer -Schneier on Security

https://www.schneier.com/blog/archives/2022/02/breaking-245-bit-elliptic-curve-encryption-with-a-quantum-computer.html

This analysis details the projected requirements for breaking modern elliptic -curve encryption, a key component of mobile and internet security. It underscores the concrete, measurable nature of the quantum threat, compelling businesses to take the migrat ion to PQC seriously.

26. Researchers Say Here's How to Prepare Now For Post Quantum Cybersecurity

https://thequantuminsider.com/2024/11/30/researchers-say-heres-how-to-prepare-now-for-post-quantum-cybersecurity/

This article emphasizes proactive steps businesses must take to prepare for the quantum transition, such as creating cryptographic inventories and developing crypto agility. The core message for executives is that preparation can and should begin now, even before the new standards are fully mandated.

27. Post-Quantum Cryptography Is a Must to Protect Your Systems | Gartner

https://www.gartner.com/en/articles/post-quantum-cryptography

Gartner, a leading business technology advisor, identifies PQC as an essential security measure for protecting systems and data with a long shelf life. This strong recommendation provides executives with a clear justification for prioritizing and funding PQC migration projects.

28. Cyber Insights 2025: Quantum and the Threat to Encryption - Security Week

https://www.securityweek.com/cyber-insights-2025-quantum-and-the-threat-to-encryption/

This forward looking analysis positions the quantum threat as a major cybersecurity issue for 2025 and beyond. It serves as a clear signal to executives that PQC is no longer a future concern but a present -day strategic imperative.

SECTION 06

Timelines and Standardization Efforts

29. What Is Post-Quantum Cryptography? | NIST

https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

This official NIST resource defines PQC and explains its role in protecting against future threats. For businesses, this is the authoritative source for understanding the Government led solution to the quantum problem and the importance of aligning with the forthcoming standards.

30. The Quantum Threat Timeline: Why Organizations Must Act Now ...

https://www.evolutionq.com/post/the-quantum-threat-timeline-why-organizations-must-act-now

This analysis presents expert timelines for the arrival of a cryptographically relevant quantum computer, creating a clear sense of urgency. The key takeaway for businesses is that the "harvest now, decrypt later" threat requires action today, regardless of the precise date of "Q-Day."

31. NIST recommends timelines for transitioning cryptographic ...

https://pqshield.com/nist-recommends-timelines-for-transitioning-cryptographic-algorithms/

This article outlines NIST's official recommended timelines for migrating away from vulnerable algorithms. These timelines provide businesses with a clear, authoritative roadmap for planning their PQC transition and ensuring compliance with Federal guidance.

32. The timelines: when can we expect useful quantum computers?

https://introtoquantum.org/essentials/timelines/

This resource provides a balanced overview of the various expert predictions for when powerful quantum computers will be built. For strategic planning, it highlights that while dates vary, the consensus is that the threat is on a foreseeable horizon, making procrastination a risky strategy.

33. 2023 Quantum Threat Timeline Report Published - Marin Ivezic

https://postquantum.com/industry-news/quantum-threat-timeline-report/

This report synthesizes expert opinions on the quantum timeline, providing a probabilistic forecast for the arrival of a CRQC. This data driven approach helps executives frame the quantum threat as a measurable business risk that requires a formal mitigation plan.

34. A Comprehensive Guide to Quantum-Resistant Cryptography and Encryption - Entrust

https://www.entrust.com/resources/learn/post-quantum-cryptography-and-encryption

This guide provides a thorough overview of PQC, covering the threat, the solutions, and the migration process. It serves as an excellent resource for executives and their teams to build a comprehensive understanding of the entire PQC challenge and its sol utions.

35. Post-quantum cryptography: A status report - CompTIA

https://production-central-www.comptia.org/blog/post-quantum-cryptography-a-status-report

This report provides a snapshot of the current state of PQC development and standardization. It gives executives a timely update on the maturity of the solutions and the progress of the global effort to create a quantum -safe ecosystem.

36. When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret | RAND

https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html

This commentary from the RAND Corporation argues that the arrival of a CRQC will likely be a public event, not a secret weapon. However, it stresses that the "harvest now, decrypt later" threat means the danger period has already begun, requiring immediate action to protect long term secrets.

37. Quantum Computing is a Long-Term Cybersecurity Risk, But Deserves Immediate Attention, Analysts Report

https://thequantuminsider.com/2025/02/01/quantum-computing-is-a-long-term-cybersecurity-risk-but-deserves-immediate-attention-analysts-report/

This report positions the quantum threat as an urgent priority for immediate action, despite being a long- term risk. For leaders, this justifies allocating resources now for discovery and planning to avoid catastrophic costs and disruptions later.

38. 10 seconds to break: Preparing for quantum security threats | Unisys

https://www.unisys.com/blog-post/cis/10-seconds-to-break-preparing-for-quantum-security-threats/

The stark headline emphasizes the speed at which a mature quantum computer could break current encryption, framing the threat in clear, impactful terms. This serves as a powerful call to action for executives to prioritize quantum readiness before today's protections become worthless.

39. How Far Away Is The Quantum Threat? - BTQ

https://www.btq.com/blog/how-far-away-is-the-quantum-threat

This article explores the different timelines and factors influencing the arrival of a CRQC. It reinforces the executive level need for proactive risk management in the face of an uncertain but high impact threat.

40. Quantum Cryptography - Shor's Algorithm Explained - Classiq

https://www.classiq.io/insights/shors-algorithm-explained

This piece provides another clear explanation of Shor's algorithm, the key to breaking public key encryption. Reinforcing this fundamental concept helps business leaders understand the specific, non - negotiable reason for the PQC transition.

41. Post-Quantum Cryptography: It's already here and it's not as scary as it sounds - Medium

https://medium.com/@dave1010/post-quantum-cryptography-its-already-here-and-it-s-not-as-scary-as-it-sounds-cb8ea70e8f1c

This article aims to demystify PQC and reduce the fear associated with the transition by focusing on the practical steps organizations can take. It provides a message of reassurance for leaders that the quantum problem, while serious, is solvable with proactive planning.

42. Understanding Quantum Threats | How to Secure Data with PQC - AppViewX

https://www.appviewx.com/blogs/understanding-quantum-threats-and-how-to-secure-data-with-post-quantum-cryptography/

This guide links the specific quantum threats to the PQC solutions designed to counter them. It offers a clear problem and- solution framework that helps executives justify PQC investments as a direct and necessary mitigation of a well understood risk.

43. Quantum Resistant Cryptography - Quside

https://quside.com/quantum-resistant-cryptography/

This source provides an overview of quantum resistant cryptography from a solutions provider. It highlights the availability of commercial technologies and expertise to help businesses navigate the transition successfully.

44. Post-Quantum Cryptography | CSRC - NIST Computer Security Resource Center

https://csrc.nist.gov/projects/post-quantum-cryptography

This is the official homepage for NIST's PQC standardization project, making it the single most authoritative source for information on the process, timelines, and selected algorithms. All business and Government PQC strategies should be directly aligned with the information provided here.

45. NIST's post-quantum cryptography standards are here - IBM Research

https://research.ibm.com/blog/nist-pqc-standards

This announcement from a major industry player like IBM signals strong commercial support for the new NIST standards. For executives, this indicates that the new ecosystem of PQC products and services is maturing rapidly, making the transition more feasible.

46. NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

NIST's selection of an additional algorithm based on different mathematics underscores its strategy of algorithmic diversity as a hedge against future breakthroughs. This prudent approach should inform business strategies, highlighting the importance of building crypto agility.

47. Post-Quantum Cryptography: The Future of Secure Communications and the Role of Standards - AppViewX

https://www.appviewx.com/blogs/post-quantum-cryptography-the-future-of-secure-communications-and-the-role-of-standards/

This article emphasizes the critical role of standardization in creating a secure and interoperable post quantum future. It reinforces the business case for aligning with the NIST standards to ensure long term security and compatibility.

48. What is Post-Quantum Cryptography (PQC)? - Palo Alto Networks

https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc

This cybersecurity leader provides a clear definition of PQC and its importance. This serves as a strong signal to the market that PQC is becoming a mainstream security requirement that businesses must address.

49. CBP Tackles Post-Quantum Cryptography | U.S. Customs and Border Protection

https://www.cbp.gov/newsroom/spotlights/cbp-tackles-post-quantum-cryptography

This article showcases a major Federal agency actively preparing for the PQC transition. It serves as a case study and a clear indication of the seriousness of the Federal mandate, signaling to contractors that PQC readiness is becoming a requirement for doing business with the Government.

SECTION 07

Industry Use Cases and Impact

50. www.bis.org

https://www.bis.org/publ/bppdf/bispap149.pdf

This report from the Bank for International Settlements details experiments with PQC in global payment systems. It demonstrates that the financial sector is taking the quantum threat seriously and provides a blueprint for how other critical infrastructure sectors can begin to prepare.

51. Impact of Quantum Computing on Finance Sector - CIO Influence

https://cioinfluence.com/it-and-devops/impact-of-quantum-computing-on-finance-sector/

This article details the profound impact quantum computing will have on the financial sector, from breaking current transaction security to enabling new forms of high speed analysis. It highlights the dual nature of quantum as both a major risk and a pote ntial opportunity for the industry.

52. What is quantum computing and how might it impact financial services?

https://www.lloydsbankinggroup.com/insights/what-is-quantum-computing-and-how-might-it-impact-financial-services.html

A major banking group explains the risks and opportunities of quantum computing for financial services. This perspective underscores the mainstream business recognition of the quantum threat and the need for proactive engagement with PQC solutions.

53. Quantum's Potential to Unlock Finance Insights - Booz Allen

https://www.boozallen.com/insights/ai-research/quantum-s-potential-to-unlock-finance-insights.html

This article focuses on the opportunities quantum computing presents for the finance industry, such as advanced risk modeling and optimization. It reminds executives that while the security threat is paramount, a quantum strategy should also consider the potential for competitive advantage.

54. The Positive and the Negative Impacts of Quantum Computers on the Finance Sector

https://www.digicert.com/blog/impact-of-quantum-computers-on-the-finance-sector

This piece provides a balanced view of quantum computing's impact on finance, covering both the cryptographic threat and the potential for process optimization. A sound business strategy must address both the risks of inaction and the opportunities of early adoption.

55. Quantum Computing in Medicine - MDPI

https://www.mdpi.com/2076-3271/12/4/67

This scholarly article explores the transformative potential of quantum computing in medicine, particularly in drug discovery and personalized treatment. It highlights a key industry where the long term value of data makes it a prime target for "harvest now, decrypt later" attacks, creating an urgent need for PQC.

56. Revolutionizing Healthcare: The Emerging Role of Quantum Computing in Enhancing Medical Technology and Treatment

https://pmc.ncbi.nlm.nih.gov/articles/PMC11416048/

This paper details how quantum computing can revolutionize healthcare through advanced diagnostics and treatment optimization. For executives in the healthcare sector, it underscores the immense value of the data at risk and the critical importance of imp lementing PQC to protect it.

57. How Is Quantum Computing Being Used in Healthcare? - HealthTech Magazine

https://healthtechmagazine.net/how-is-quantum-computing-being-used-in-healthcare-perfcon

This article provides practical examples of how quantum computing is being applied in healthcare today. These use cases highlight the increasing reliance on complex data, reinforcing the business case for protecting that data with quantum resistant encryption.

58. Quantum Computing for Healthcare: A Review - MDPI

https://www.mdpi.com/1999-5903/15/3/94

This academic review surveys the broad applications of quantum computing in healthcare. The sheer scope of potential transformation described in the paper makes a compelling argument for proactively securing the underlying data with PQC.

59. Quantum Computing and Quantum Technology Use Cases in Healthcare & Medical Research - Marin Ivezic

https://postquantum.com/quantum-computing/quantum-use-cases-healthcare-medical-research/

This article outlines specific use cases for quantum technology in medical research. Given the extremely long lifespan and high value of medical research data, it presents a powerful argument for why the healthcare and pharmaceutical sectors must be early adopters of PQC.

60. The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine

https://pmc.ncbi.nlm.nih.gov/articles/PMC6205278/

This paper explores the synergy between quantum computing and machine learning in medicine. The advanced analytical capabilities described highlight the creation of extremely high value intellectual property, which must be protected by quantum resistant security measures.

SECTION 08

National Security and Government

61. What Is Quantum Computing? | Council on Foreign Relations

https://www.cfr.org/backgrounder/what-quantum-computing

The Council on Foreign Relations provides a high- level briefing on quantum computing, framed in the context of international relations and national security. This perspective is essential for executives in the defense and aerospace sectors, as it situates technology as a geopolitical issue.

62. The realist's guide to quantum technology and national security - Deloitte

https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html

Deloitte offers a pragmatic guide to the impact of quantum technology on national security. It provides a clear eyed business risk assessment for defense contractors and other organizations in the national security ecosystem.

63. The impact of quantum technology on national security - ID Quantique

https://www.idquantique.com/the-impact-of-quantum-technology-on-national-security/

This article details the specific ways in which quantum technology will affect national security, from breaking codes to enabling new forms of sensing. It underscores the necessity for defense agencies and their contractors to be at the forefront of the P QC transition.

SECTION 09

Market Trends and Future Outlook

64. Quantum Computing Advances But Real-World Impact Remains Elusive: New Forrester Report - Datanami

https://www.bigdatawire.com/2025/01/10/quantum-computing-advances-but-real-world-impact-remains-elusive-new-forrester-report/

This report from Forrester provides a sober assessment of the quantum computing market, noting that practical applications are still emerging. For executives, this context suggests that while the security threat must be addressed now, the timeline for off ensive quantum capabilities provides a window for methodical migration.

65. 2025 Will See Huge Advances in Quantum Computing. So What is a Quantum Chip And How Does it Work?

https://thequantuminsider.com/2025/01/08/2025-will-see-huge-advances-in-quantum-computing-so-what-is-a-quantum-chip-and-how-does-it-work/

This article forecasts significant progress in quantum hardware for 2025. Such advances directly shorten the timeline for a CRQC, increasing the urgency for businesses to implement their PQC transition plans.

66. How Many Quantum Computers Are There in 2025? - SpinQ

https://www.spinquanta.com/news-detail/how-many-quantum-computers-are-there

This article attempts to quantify the number of quantum computers currently in existence. While the number is small, the rapid growth it implies is a key indicator for businesses that the technology is maturing and the threat timeline is shrinking.

67. Quantum computing: What leaders need to know now | MIT Sloan

https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

This article from MIT Sloan is tailored specifically for business leaders, outlining the strategic implications of quantum computing. It frames quantum readiness not just as a technical issue but as a core component of future business strategy.

68. Quantum computing's six most important trends for 2025 - Moody's

https://www.moodys.com/web/en/us/insights/quantum/quantum-computings-six-most-important-trends-for-2025.html

Moody's identifies key trends in quantum computing, providing a financial and risk -oriented perspective. This analysis is valuable for executives seeking to understand the market dynamics and investment landscape surrounding the technology.

69. 2025: The year to become Quantum-Ready - Microsoft Azure

https://azure.microsoft.com/en-us/blog/quantum/2025/01/14/2025-the-year-to-become-quantum-ready/

Microsoft, a major cloud and enterprise provider, declares 2025 as the year for businesses to become "quantum ready." This strong market signal indicates that the tools and platforms to begin the PQC transition are now available and that industry leaders expect their customers to begin acting.

70. Practical Quantum Computing Five to Ten Years Away: Google CEO

https://thequantuminsider.com/2025/02/13/practical-quantum-computing-five-to-ten-years-away-google-ceo/

The CEO of Google provides a timeline for the arrival of practical, large scale quantum computers. This forecast from a key industry leader gives businesses a credible window for planning and executing their migration to quantum resistant security.

71. Quantum Computing Market 2025-2045: Technology, Trends, Players, Forecasts - IDTechEx

https://www.idtechex.com/en/research-report/quantum-computing-market-2025/1053

This market research report provides long term forecasts for the quantum computing industry. For strategic planning and investment, this data helps companies understand the growth trajectory and potential market size of this disruptive technology.

72. Big Ideas in Quantum For 2025

https://thequantuminsider.com/2024/12/23/big-ideas-in-quantum-for-2025/

This article outlines the most significant anticipated developments in quantum computing for the coming year. Staying abreast of such forecasts allows business leaders to remain agile and adjust their quantum strategies in response to rapid technological advancements.

73. What Is Quantum Computing's Threat to Cybersecurity? - Palo Alto Networks

https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity

A leading cybersecurity company explains the quantum threat, signaling to the market that PQC is becoming a standard component of enterprise security. This reinforces the need for businesses to integrate PQC into their overall cybersecurity posture.

74. Quantum Computing's Impact on Cryptography — The Future of Encryption - Medium

https://medium.com/@RocketMeUpCybersecurity/quantum-computings-impact-on-cryptography-the-future-of-encryption-1f8804205d86

This article explores the future of encryption in a world with quantum computers. It underscores the fundamental shift that is occurring and the need for businesses to move beyond legacy systems to a new, quantum safe cryptographic foundation.

75. Assessing the Vulnerability of Current Cryptographic Protocols to Quantum Attacks

https://decentcybersecurity.eu/assessing-the-vulnerability-of-current-cryptographic-protocols-to-quantum-attacks/

This resource focuses on the process of assessing cryptographic vulnerabilities within an organization. It highlights the importance of a thorough inventory as the critical first step in any PQC migration plan.

76. Cybersecurity Quantum Attack - Identity Management Institute®

https://identitymanagementinstitute.org/cybersecurity-quantum-attack/

This article examines the specific threat that quantum attacks pose to identity and access management systems. It highlights a critical area of vulnerability for businesses that relies heavily on public key cryptography and must be prioritized in a PQC tr ansition.

77. Quantum-safe overview

https://quantum.microsoft.com/en-us/vision/quantum-cryptography-overview

Microsoft provides its high level vision for a quantum- safe future. This strategic overview from a major technology provider helps businesses understand the industry roadmap and the ecosystem of tools and platforms being built to support the transition.

78. Prevent the Latest Quantum Threats with Post Quantum Cryptography | Blogs - CyberHive

https://www.cyberhive.com/insights/prevent-the-latest-quantum-threats-with-post-quantum-cryptography/

This blog post frames PQC as a direct and necessary countermeasure to emerging quantum threats. It reinforces the simple business case that proactive PQC adoption is a sound investment in risk mitigation.

79. Introduction to Quantum-Safe Cybersecurity: Why SEBI-Regulated Entities Should Care

https://www.qnulabs.com/blog/introduction-to-quantum-safe-cybersecurity-why-sebi-regulated-entities-should-care

This article targets a specific regulated industry, explaining why quantum -safe cybersecurity is a compliance and risk management imperative. It serves as an example of how PQC is becoming a sector - specific regulatory concern that businesses must address.

80. Post-Quantum Security: Is Your Encryption Obsolete? - Devoteam

https://www.devoteam.com/expert-view/post-quantum-security-is-your-encryption-obsolete/

Posing a direct question to business leaders, this article argues that current encryption systems are effectively obsolete due to the future quantum threat. This framing encourages executives to view their legacy cryptographic systems as a form of technical debt that must be addressed.

81. Preparing for Quantum-Safe Cryptography in IT Systems - Com Pro Business Solutions

https://www.comprobusiness.com/insights/preparing-for-quantum-safe-cryptography-in-it-systems/

This article provides practical advice on preparing IT systems for the transition to PQC. It helps bridge the gap between high level strategy and the concrete technical steps required for implementation.

82. Quantum Computing: The Urgent Need to Transition to Quantum-Resistant Cryptography

https://bpi.com/quantum-computing-the-urgent-need-to-transition-to-quantum-resistant-cryptography/

This source emphasizes the urgency of the PQC transition, likely from a business or policy perspective. It serves to reinforce the message to executives that procrastination is a high risk strategy.

83. Securing the Future with Quantum-Safe Cryptography - Guidehouse

https://guidehouse.com/insights/advanced-solutions/2025/quantum-safe-cryptography

A major consulting firm outlines the path to a quantum -safe future, signaling that PQC migration has become a key strategic advisory service. This indicates a maturing market for PQC implementation and a clear signal that businesses should be seeking expert guidance.

84. Kicking off your quantum migration program - National Cyber Security Centre

https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2024/march/25/quantum-secure/Make+your+organization+quantum+secure.pdf

This guide from a national cybersecurity agency provides an official, Government -backed framework for starting a PQC migration. It offers an authoritative roadmap that businesses can adopt for their own planning and execution.

85. The looming threat of quantum computing to data security - Fractal Analytics

https://fractal.ai/nists-post-quantum-cryptographic-standards/

This article connects the quantum threat directly to the importance of the NIST standards. It helps executives understand that the solution to the problem is not arbitrary but is driven by a rigorous, internationally recognized standardization process.

86. Quantum-Safe Networks — Can We Future-Proof Data Security? - Medium

https://medium.com/@RocketMeUpCybersecurity/quantum-safe-networks-can-we-future-proof-data-security-ea8a89d14e83

This article explores the concept of building quantum safe networks as a way to ensure long term data security. For business leaders, it shifts the conversation from a one- time fix to an ongoing strategy of building a resilient and future -proofed security architecture.

87. Quantum-Safe Cryptography (QSC) - ETSI

https://www.etsi.org/technologies/quantum-safe-cryptography

The European Telecommunications Standards Institute (ETSI) provides its own overview of QSC, highlighting the international and cross industry nature of the PQC transition. This shows that the move to quantum -safe standards is a global effort, not just a U.S.-based initiative.

SECTION 10

PQC Standards and Implementation

88. An overview of Quantum Cryptography and Shor's Algorithm - Warse

https://www.warse.org/IJATCSE/static/pdf/file/ijatcse214952020.pdf

This paper offers a formal overview of quantum cryptography, focusing on Shor's algorithm as the primary driver of the current security transition. It serves as a technical foundation for any business' internal documentation on why PQC migration is necessary.

89. Transitioning to Quantum-Safe Encryption - Delinea

https://delinea.com/blog/quantum-safe-encryption

This article focuses on the practical steps and strategies for transitioning to quantum safe encryption. It moves the conversation from the "why" to the "how," providing actionable insights for business and IT leaders tasked with executing the migration.

90. Quantum-Safe Infrastructure: Tough Challenges (And Expert Solutions) -Forbes

https://www.forbes.com/councils/forbestechcouncil/2025/01/24/quantum-safe-infrastructure-tough-challenges-and-expert-solutions/

This article discusses the challenges of building a quantum safe infrastructure and points toward available expert solutions. For executives, it frames the PQC transition as a complex but manageable project that can be successfully outsourced or supported by specialized vendors.

91. The Impact of Quantum-Safe Cryptography (QSC) on Website Response -arXiv

https://arxiv.org/html/2411.05024v1

This technical paper analyzes the performance impact of post quantum cryptography on website response times, noting a measurable but manageable increase in latency. This data is critical for business leaders to set realistic performance expectations during and after the PQC migration.

92. Post-Quantum Cryptography — Preparing for a Quantum-Resistant Future | by RocketMe Up Cybersecurity | Medium

https://medium.com/@RocketMeUpCybersecurity/post-quantum-cryptography-preparing-for-a-quantum-resistant-future-a3810536dcd8

This article serves as a guide for businesses preparing for the transition to a quantum resistant future. It emphasizes the need for proactive planning and provides a roadmap for achieving a secure cryptographic posture.

93. Is Quantum Computing a Cybersecurity Threat? | American Scientist

https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat

This article from a respected scientific publication confirms that quantum computing does pose a significant and credible threat to cybersecurity. This authoritative validation helps business leaders communicate the seriousness of the issue to boards and stakeholders.

94. Quantum-Safe Cryptography - Medium

https://medium.com/@kumarshivam-66534/quantum-safe-cryptography-26bd886737e1

This article provides another overview of quantum safe cryptography, reinforcing its importance as the necessary solution to the quantum threat. The consistent messaging across multiple sources strengthens the case for immediate executive action.

95. Quantum's Impact on Cybersecurity: The Hero and Villain - Viva Technology

https://vivatechnology.com/news/quantum-s-impact-on-cybersecurity

This piece presents a dual perspective, framing quantum technology as both a threat to current security (villain) and a potential tool for new, more powerful defenses (hero). A comprehensive business strategy should explore both mitigating the risks and harnessing the opportunities.

96. Trailblazers in Quantum -Safe Networks: Which Industries Are Paving the Way?

https://www.thefastmode.com/expert-opinion/39774-trailblazers-in-quantum-safe-networks-which-industries-are-paving-the-way

This article highlights the industries, such as finance and telecommunications, that are leading the adoption of quantum safe networks. These case studies provide valuable models and best practices for businesses in other sectors to follow.

97. Timelines for migration to post-quantum cryptography - NCSC.GOV.UK

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

The UK's National Cyber Security Centre provides its official timelines for migrating to PQC. This guidance from a major international partner demonstrates the global consensus on the quantum threat and the need for a coordinated transition.

98. UK sets timeline for country's transition to quantum-resistant encryption -The Record

https://therecord.media/uk-ncsc-quantum-resistant-algorithms-transition

This news article reports on the UK's official PQC transition timeline, making the information more accessible to a general business audience. It underscores the international regulatory momentum that will soon impact global supply chains and business partnerships.

99. What is Quantum-Safe Cryptography? - IBM

https://www.ibm.com/think/topics/quantum-safe-cryptography

IBM offers a clear definition and overview of quantum - safe cryptography. As a major enterprise technology provider, its focus on this topic signals to business customers that PQC is becoming a core component of the modern IT ecosystem.

100. DORA and your quantum-safe cryptography migration - IBM

https://www.ibm.com/think/insights/dora-quantum-safe-cryptography-migration

This article connects the PQC migration to existing financial services regulations like DORA (Digital Operational Resilience Act). It provides a compelling example of how PQC is not just a future security issue but is becoming an immediate regulatory and compliance concern.

101. Migrating to quantum-safe infrastructure - ID Quantique

https://www.idquantique.com/quantum-safe-security/migrating-to-quantum-safe-infrastructure/

This resource from a specialized vendor outlines the process and solutions for migrating to a quantum safe infrastructure. It demonstrates that a mature market of tools and expertise exists to support businesses through this complex transition.

SECTION 11

Business Risks and Impacts

102. Data Breaches Cause A Financial Burden - Cyber Security Intelligence

https://www.cybersecurityintelligence.com/blog/data-breaches-cause-a-financial-burden-8297.html

This article details the significant financial costs associated with data breaches. In the quantum context, it serves as a stark reminder of the massive financial and reputational damage a quantum attack could inflict, making proactive PQC investment a sound financial decision.

103. Securing our digital future against quantum threats | Technology Innovation Institute - TII

https://www.tii.ae/insights/securing-our-digital-future-against-quantum-threats

This article frames the PQC transition as a critical step in securing the entire digital future. For executives, it elevates the issue from a simple technical upgrade to a strategic imperative for long term business survival.

104. What Are the Implications of Quantum Computing for the Future of Data Security? | socPub

https://socpub.com/articles/what-are-implications-quantum-computing-future-data-security-17926

This piece explores the broad implications of quantum computing for data security. It prompts business leaders to consider not only the immediate threat but also the long term changes to compliance, data governance, and risk management.

105. Report Estimates Trillions in Indirect Losses Would Follow Quantum Computer Hack

https://www.nextgov.com/cybersecurity/2023/05/report-estimates-trillions-indirect-losses-would-follow-quantum-computer-hack/386653/

This article quantifies the potential economic fallout of a large -scale quantum attack in the trillions of dollars. This staggering figure provides a powerful justification for executives to secure the necessary budget and resources for a comprehensive PQ C migration.

106. What Impact Does Data Breaches Have On Reputation? - Sustainability Directory

https://sustainability-directory.com/question/what-impact-does-data-breaches-have-on-reputation/

This article discusses the severe reputational damage that results from data breaches. A future quantum breach would be catastrophic to a company's brand and customer trust, making proactive PQC adoption a critical component of reputation management.

107. Data Breach Notification Laws and the Quantum Decryption Problem

https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4765&context=wlulr

This legal analysis explores how "harvest now, decrypt later" attacks create complex new challenges for data breach notification laws. It highlights the significant legal and compliance risks businesses face if they fail to protect long- term data with PQC .

108. What are the legal implications of security breaches? - Nucamp

https://www.nucamp.co/blog/coding-bootcamp-full-stack-web-and-mobile-development-what-are-the-legal-implications-of-security-breaches

This article outlines the serious legal consequences of security breaches, including fines, lawsuits, and regulatory penalties. The scale of a potential quantum breach makes it a top tier legal risk that requires board level attention and a robust PQC mit igation strategy.

109. CIOs must prepare their organizations today for quantum -safe cryptography

https://www.scquantum.org/news/cios-must-prepare-their-organizations-today-quantum-safe-cryptography

This article issues a direct call to action for Chief Information Officers to begin preparing for PQC immediately. It positions quantum readiness as a key leadership responsibility and a critical component of modern IT governance.

SECTION 12

Industry Solutions and Readiness

110. The state of the post-quantum Internet - The Cloudflare Blog

https://blog.cloudflare.com/pq-2024/

Cloudflare, a major internet infrastructure provider, reports on its progress in deploying PQC across its global network. This demonstrates that the PQC transition is technically feasible at scale and is already underway at the core of the internet.

111. Cloudflare Advances Industry's First Cloud -Native Quantum-Safe Zero Trust Solution

https://www.stocktitan.net/news/NET/cloudflare-advances-industry-s-first-cloud-native-quantum-safe-zero-f8n5nm073puy.html

This press release announces a specific, commercially available quantum -safe security solution. It serves as a clear market signal that PQC products are moving from development to deployment, enabling businesses to begin their implementation.

112. Q-Day: Estimating and Preparing for Quantum Disruption in Cybersecurity | Secureworks

https://www.secureworks.com/blog/predicting-q-day-and-impact-of-breaking-rsa2048

This article from a cybersecurity firm focuses on "Q-Day", the day a CRQC arrives, and outlines how businesses can prepare. It provides a practical, risk based framework for executives to plan and execute their PQC migration strategy.

113. Quantum Security In Telecommunications - ID Quantique

https://www.idquantique.com/quantum-safe-security/quantum-security-in-telecommunications/

This piece focuses on the critical need for quantum security within the telecommunications sector. It highlights a key infrastructure area where PQC is essential for national security and the functioning of the digital economy.

114. Nokia and Turkcell Demonstrate Industry Leading Quantum-Safe Protection for Mobile Subscribers

https://www.nokia.com/about-us/news/releases/2024/12/20/nokia-and-turkcell-demonstrate-industry-leading-quantum-safe-protection-for-mobile-subscribers/

This press release announces a successful real- world trial of PQC in a mobile network. Such pilots are crucial to building confidence in technology and demonstrating its readiness for widespread commercial deployment.

115. Types of Post Quantum Cryptography Public Key Schemes - Utimaco

https://utimaco.com/news/blog-posts/types-post-quantum-cryptography-public-key-schemes

This article breaks down the different families of PQC algorithms. For business leaders, this overview helps in understanding that PQC is not a single technology but a portfolio of solutions that can be chosen to best fit specific performance and security needs.

116. Post-quantum cryptography: Lattice-based cryptography - Red Hat

https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography

Red Hat, a leading enterprise software company, explains the importance of lattice based cryptography. Their endorsement signals strong support for the NIST standards within the open source and enterprise software ecosystems.

117. What is lattice- based cryptography? | Sectigo® Official

https://www.sectigo.com/resource-library/what-is-lattice-based-cryptography

A leading digital certificate authority explains lattice -based cryptography. This is significant because it shows that the core infrastructure of internet trust (i.e., certificate authorities) is actively preparing to support and issue PQC - based certifica tes.

118. Limitations of Post Quantum Cryptography | Encryption Consulting

https://www.encryptionconsulting.com/education-center/limitations-of-post-quantum-cryptography/

This article discusses the potential drawbacks of PQC, such as larger key sizes and higher performance overhead. A balanced business strategy must account for these limitations and plan for potential infrastructure upgrades or architectural changes.

119. What is Hash-based Cryptography? - Utimaco

https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-hash-based-cryptography

This piece explains the mechanics and benefits of hash -based cryptography. For executives, the key takeaway is that this type of PQC offers strong security guarantees, making it an excellent choice for high- value applications like firmware signing.

120. What is Code-based Cryptography? - Utimaco

https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-code-based-cryptography

This article describes code based cryptography, the foundation for HQC, which NIST selected as an alternative PQC standard. This reinforces the importance of algorithmic diversity and having multiple, distinct quantum safe options available.

121. Code-Based Cryptography: State of the Art and Perspectives - IEEE Computer Society

https://www.computer.org/csdl/magazine/sp/2017/04/msp2017040044/13rRUxASuo3

This academic paper provides a deep dive into the state of code based cryptography. It offers technical validation for the security of this PQC approach, building confidence for its use in critical systems.

122. CBCrypto

https://www.cb-crypto.org/

This is the website for a conference on code based cryptography. The existence of specialized academic conferences demonstrates a mature and active research community behind this family of PQC algorithms.

123. Demystifying Multivariate Cryptography - NCC Group

https://www.nccgroup.com/us/research-blog/demystifying-multivariate-cryptography/

A cybersecurity consultancy explains multivariate cryptography. This type of analysis from security professionals helps businesses understand the pros and cons of different PQC approaches beyond the final NIST selections.

124. Post-Quantum Cryptography: 2024 Standards Explained - Qrypt

https://www.qrypt.com/resources/2024-post-quantum-cryptography-standards-explained/

This resource explains the NIST standards that were finalized in 2024. Clear, accessible explanations like this are valuable tools for educating internal teams and stakeholders about the specific solutions being deployed.

125. Quantum Threats to Identity and Access Management

https://identitymanagementinstitute.org/quantum-threats-to-identity-and-access-management/

This article focuses on the specific risk quantum computing poses to identity systems, which are foundational to enterprise security. It highlights an area of critical vulnerability that must be a top priority in any PQC migration plan.

126. The Cost of Quantum Safety Implementing Post-Quantum Cryptography | Women in Tech Network

https://www.womentech.net/how-to/cost-quantum-safety-implementing-post-quantum-cryptography

This article explores the potential costs associated with migrating to PQC. Understanding these costs, from software and hardware to personnel and training, is an essential first step for executives in budgeting and planning for the transition.

SECTION 13

Market and Vendor Landscape

127. 10 Leading Quantum Computing Companies at the Forefront - BlueQubit

https://www.bluequbit.io/quantum-computing-companies

This article lists the top companies in the quantum computing space. For business leaders, this provides a snapshot of the key players, both potential partners and sources of disruption in the rapidly developing quantum ecosystem.

128. Quantum Threats Are Accelerating -- These Companies Are Preparing for the Shift

https://www.newswire.ca/news-releases/quantum-threats-are-accelerating-these-companies-are-preparing-for-the-shift-887987796.html

This press release highlights that multiple companies are already taking concrete steps to prepare for the quantum threat. This market movement serves as a strong signal that PQC is becoming a competitive differentiator and a standard feature of enterprise grade security.

129. Quantum Technologies Investment Landscape Report 2025-2045, - GlobeNewswire

https://www.globenewswire.com/news-release/2025/03/21/3046976/0/en/Quantum-Technologies-Investment-Landscape-Report-2025-2045-with-Profiles-of-300-Companies-Across-the-Quantum-Technology-Landscape-Analysis-of-Start-ups-Tech-Giants-and-Public-priva.html

This report analyzes the investment landscape for quantum technologies, providing valuable market intelligence. For executives, this data can inform strategic decisions about investment, partnership, and acquisition in the quantum space.

130. Quantum Safe | IBM Quantum Computing

https://www.ibm.com/quantum/quantum-safe

This is IBM's official portal for its quantum safe solutions. It represents a clear, commercially supported pathway for enterprises to begin their PQC transition with tools and services from a major, trusted vendor.

131. SEALSQ Strengthens Its Quantum-Safe Roadmap by Allocating Up To $20 Million Into Cutting-Edge Startup Investments

https://www.sealsq.com/investors/news-releases/sealsq-strengthens-its-quantum-safe-roadmap-by-allocating-up-to-20-million-into-cutting-edge-startup-investments

This announcement shows a security company actively investing in the PQC ecosystem. This type of M&A and investment activity signals a maturing and consolidating market for quantum safe solutions.

132. Post-Quantum Cryptography Market Set for Accelerated Growth as SEALSQ and WISeKey Lead the Way in Securing Digital Infrastructure

https://www.sealsq.com/investors/news-releases/post-quantum-cryptography-market-set-for-accelerated-growth-as-sealsq-and-wisekey-lead-the-way-in-securing-digital-infrastructure

This press release forecasts accelerated growth in the PQC market. This provides a strong signal to executives that PQC is not just a compliance requirement but also a significant new market opportunity.

133. Is quantum computing a threat to crypto? - Coinbase

https://www.coinbase.com/learn/crypto-basics/is-quantum-computing-a-threat-for-crypto

Coinbase, a major cryptocurrency exchange, addresses the quantum threat to digital assets. The fact that the cryptocurrency industry is actively planning for PQC demonstrates the seriousness of the threat to any system that relies on public key cryptography for security and value.

SECTION 14

Technical Implementation and Analysis

134. Implementation and Analysis of Shor's Algorithm to Break RSA Cryptosystem Security - TechRxiv

https://www.techrxiv.org/users/708580/articles/693052/master/file/data/RESERCH%20FINAL/RESERCH%20FINAL.pdf

This technical paper details a practical implementation of Shor's algorithm. While academic, it provides concrete proof of the algorithm's viability, moving it from a theoretical threat to a demonstrable one.

135. The Emerging Potential for Quantum Computing in Irregular Warfare

https://irregularwarfarecenter.org/publications/insights/the-emerging-potential-for-quantum-computing-in-irregular-warfare/

This article explores the national security implications of quantum computing beyond traditional code breaking, including its use in irregular warfare. This broader context is crucial for executives in the defense and intelligence sectors to consider in their strategic planning.

136. Implementation and Analysis of Shor's Algorithm to Break RSA Cryptosystem Security

https://www.authorea.com/users/708580/articles/693052-implementation-and-analysis-of-shor-s-algorithm-to-break-rsa-cryptosystem-security

Similar to the TechRxiv paper, this academic article provides a detailed analysis of implementing Shor's algorithm. Repeated, independent confirmation of the algorithm's feasibility across the research community solidifies the certainty of the threat.

137. Quantum Computing's Impact on Cybersecurity and the Road Ahead - SecureWorld

https://www.secureworld.io/industry-news/quantum-computing-impact-cybersecurity

This article provides a high level overview of quantum's impact on cybersecurity and outlines the path forward for businesses. It's a good introductory resource for executives beginning to formulate their PQC strategy.

138. Quantum is coming — and bringing new cybersecurity threats with it - KPMG International

https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html

A major global consulting firm, KPMG, analyzes the cybersecurity threats from quantum computing. This type of analysis from a "Big Four" firm signals that PQC has become a mainstream business risk and a key topic for board level discussions and audits.

139. How Shor's Algorithm Breaks RSA: A Quantum Computing Guide - SpinQ

https://www.spinquanta.com/news-detail/shors-algorithm

This guide offers another clear explanation of the mechanics behind Shor's algorithm. The availability of numerous such explainers from various vendors indicates a mature understanding of the problem and a focus on educating the market about the solutions.

140. Shor's Algorithm and RSA Encryption

https://www.qai.ca/resource-library/shors-algorithm-and-rsa-encryptionnbsp

This resource directly links the specific algorithm (Shor's) to the specific vulnerability (RSA encryption). This direct causal link is the core of the business case for migrating to PQC.

141. Quantum computing concerns & positive impacts - Sectigo

https://www.sectigo.com/resource-library/quantum-computing-concerns-positive-impacts

This article from a certificate authority provides a balanced view of both the risks and the opportunities of quantum computing. This dual perspective is essential for a holistic business strategy that both mitigates threats and seeks competitive advantage.

142. Post-Quantum Cryptography: Implications of Google's Willow - Accutive Security

https://accutivesecurity.com/post-quantum-cryptography-the-implications-of-googles-willow-and-other-quantum-computers-for-cybersecurity/

This article discusses the implications of specific quantum hardware developments, like Google's "Willow" chip, for cybersecurity. It connects the abstract threat of PQC to concrete, real -world hardware milestones, making the threat more tangible for business leaders.

SECTION 15

Government and Policy

143. The Next Big Cyber Threat Could Come from Quantum Computers… Is the Government Ready? - GAO

https://www.gao.gov/blog/next-big-cyber-threat-could-come-quantum-computers-government-ready

This blog post from the Government Accountability Office (GAO) poses a direct question about the Federal Government's readiness for the quantum threat. It signals that PQC migration is a major issue of Government efficiency and national security, subject to oversight and audits.

144. Quantum Technology Challenge: What Role for the Government?

https://www.businessofgovernment.org/blog/quantum-technology-challenge-what-role-government

This article explores the role of the Government in navigating the challenges of quantum technology. It provides context for the Federal mandates and standardization efforts, showing them as part of a broader national strategy.

145. Anticipating the Quantum Threat to Cryptography | HP Wolf Security

https://threatresearch.ext.hp.com/anticipating-the-quantum-threat-to-cryptography/

HP, a major hardware and enterprise solutions provider, analyzes the quantum threat. Their focus on this issue indicates that PQC is becoming a consideration for endpoint and hardware security, not just for networks and software.

146. How Businesses Can Prepare For Quantum Threats With Post-Quantum Cryptography - Forbes

https://www.forbes.com/councils/forbesbusinesscouncil/2025/01/14/how-businesses-can-prepare-for-quantum-threats-with-post-quantum-cryptography/

This Forbes article provides actionable advice for businesses on how to prepare for the quantum threat. Its presence in a major business publication underscores that PQC readiness is now a mainstream business topic.

147. Post-Quantum Cryptography (PQC) - Challenges and obstacles to adoption | IDEMIA

https://www.idemia.com/insights/key-obstacles-post-quantum-cryptography-pqc-adoption

This article focuses on the practical challenges and obstacles to adopting PQC, such as cost, complexity, and lack of awareness. Understanding these hurdles is the first step for executives in developing a realistic and successful migration plan.

148. Quantum Computers—the Ultimate Blessing & Curse for the US Gov't? - GovCon Wire

https://www.govconwire.com/2025/01/quantum-computers-impact-us-gov-gil-herrera-nsa/

This article discusses the dual nature of quantum computing for the U.S. Government. For Government contractors, it highlights the significant business opportunities in providing both defensive PQC solutions and offensive quantum capabilities.

149. Call for action: urgent plan needed to transition to post-quantum cryptography together

https://www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together

Europol, the European Union's law enforcement agency, issues an urgent call for a coordinated transition to PQC. This highlights the global and law enforcement consensus on the quantum threat, adding to the pressure on businesses to act.

150. From the Frontlines of Post-Quantum Cryptography - Booz Allen

https://www.boozallen.com/insights/velocity/from-the-frontlines-of-post-quantum-cryptography.html

A major Government contractor, Booz Allen, shares its experiences from the "frontlines" of PQC implementation. This provides valuable real world insights for other organizations, particularly those in the public sector and defense industrial base.

151. Why post-quantum security planning must start today - Washington Technology

https://www.washingtontechnology.com/opinion/2025/03/why-post-quantum-security-planning-must-start-today/403692/

This article, aimed at Government contractors, argues that PQC planning must begin immediately. It signals that quantum readiness is becoming a key factor in Government procurement and a competitive differentiator for contractors.

152. Technology Security - National Quantum Initiative

https://www.quantum.gov/security/

This is the official page for the security aspects of the U.S. National Quantum Initiative. It serves as a central hub for understanding the Government's official strategy and policies regarding the quantum threat.

153. FACT SHEET: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future | OSTP | The White House

https://bidenwhitehouse.archives.gov/ostp/news-updates/2024/08/13/fact-sheet-biden-harris-administration-continues-work-to-secure-a-post-quantum-cryptography-future/

This official White House fact sheet outlines the administration's actions and policies regarding PQC. It is a definitive source that confirms the high level of political commitment to the PQC transition, creating a strong mandate for both Federal agencies and their contractors.

154. Post-Quantum Cryptography Initiative | CISA

https://www.cisa.gov/quantum

This is the official homepage for CISA's PQC initiative. It is a critical resource for businesses seeking to align with Federal guidelines and understand the specific services and information CISA provides to support the transition.

155. White House: Agencies Need $7.1B to Transition to PQC - MeriTalk

https://www.meritalk.com/articles/white-house-agencies-need-7-1b-to-transition-to-pqc/

This article reports on the White House's official cost estimate for the Federal PQC transition. This figure not only highlights the scale of the undertaking but also signals the significant market opportunity for vendors providing PQC solutions and servi ces.

156. REPORT ON POST-QUANTUM CRYPTOGRAPHY

https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

This is a link to an official White House report on PQC. Such reports provide the detailed justification and strategic framework behind Government mandates, offering valuable insights for business planning and alignment.

157. What is the cyber security risk from quantum computing? - KPMG ...

https://kpmg.com/au/en/home/insights/2024/04/cyber-security-risk-from-quantum-computing.html

This analysis from KPMG details the cybersecurity risks of quantum computing from a business advisory and audit perspective. It's a clear signal that PQC is becoming a key issue for corporate governance, risk, and compliance.

158. The Financial Market's Transition to Post-Quantum Cryptography - PQShield

https://pqshield.com/publications/the-financial-markets-transition-to-post-quantum-cryptography/

This report focuses specifically on the PQC transition within the financial markets. It provides a detailed case study of a critical infrastructure sector that is actively grappling with the quantum threat, offering lessons for other industries.

159. The Post-Quantum Cryptography Race: How Prepared Are Governments Globally?

https://publicsectornetwork.com/insight/the-post-quantum-cryptography-race-how-prepared-are-governments-globally

This article compares the PQC readiness of Governments around the world. For multinational corporations, this global perspective is crucial for understanding the varying regulatory landscapes and timelines they will face in different regions.

160. US Government Quantum Timeline - QuSecure

https://www.qusecure.com/us-government-quantum-timeline/

This resource consolidates the various U.S. Government PQC timelines into a single view. It is a valuable tool for executives and program managers seeking to understand the key deadlines and milestones that will drive their compliance and migration effort s.

161. Post Quantum Cryptography: An Urgent Global Cybersecurity Imperative - Forescout

https://www.forescout.com/blog/post-quantum-cryptography-an-urgent-global-cybersecurity-imperative/

This article from a network security company frames PQC as an urgent global imperative. It reflects the growing consensus within the cybersecurity industry that PQC is a necessary evolution of digital defense.

162. Post Quantum Cryptography algorithms explained - Quside

https://quside.com/post-quantum-cryptography-algorithms-explained/

This source provides another clear explanation of the different types of PQC algorithms. The proliferation of such explainers indicates a market that is actively trying to educate customers and simplify a complex technical topic for business decision makers.

163. Post quantum cryptography | Cloudflare

https://www.cloudflare.com/pqc/

This is Cloudflare's main portal for its PQC initiatives. It showcases their commitment to deploying quantum safe technologies at the internet's core, giving businesses confidence that the underlying infrastructure is being secured.

164. Securing data in the post-quantum age - PwC

https://www.pwc.com/m1/en/publications/securing-data-in-the-post-quantum-age.html

PwC, a major global advisory firm, provides its perspective on securing data in the post quantum age. Their focus on this topic reinforces that PQC has become a key element of corporate strategy and risk management.

165. White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post - Quantum Cryptography Migration

https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/

This news report amplifies the White House's cost estimate for the PQC transition. Reporting in the trade press ensures this information reaches a wide audience of Government and industry leaders, highlighting the scale of the challenge and opportunity.

166. UK Sets Timeline, Road Map for Post-Quantum Cryptography Migration

https://thequantuminsider.com/2025/03/20/uk-sets-timeline-road-map-for-post-quantum-cryptography-migration/

This article reports on the UK's official roadmap for PQC migration. It provides further evidence of the coordinated, international effort to address the quantum threat and helps multinational businesses plan their global transition strategies.

167. US Government estimates a spend of $7.1bn on PQC - PQShield

https://pqshield.com/the-white-house-report-on-post-quantum-cryptography/

A PQC vendor reports on the U.S. Government's estimated spending, directly connecting the Federal mandate to market opportunities. This highlights the business case for investing in PQC product development and services.

168. Quantum Computing and Critical Infrastructure: PQC Is Released, What Now?

https://thequantuminsider.com/2024/10/16/quantum-computing-and-critical-infrastructure-pqc-is-released-what-now/

This article explores the next steps for protecting critical infrastructure now that the first PQC standards have been released. It moves the conversation from standardization to implementation, which is the key focus for business leaders.

169. Post-Quantum Considerations for Operational Technology - CISA

https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf

This is an official CISA document focusing on the PQC challenges within Operational Technology (OT) environments like industrial control systems. It is a critical resource for businesses in the manufacturing, energy, and utility sectors.

170. Quantum Cybersecurity Explained: Comprehensive Guide

https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/

This guide provides a broad overview of the entire field of quantum cybersecurity. It's a useful starting point for executives who need to get up to speed on all the key concepts, from the threat to the solutions.

171. NISTIR 8547: PQC Standards to Real Implementations | CSA - Cloud Security Alliance

https://cloudsecurityalliance.org/blog/2025/03/20/nistir-8547-from-pqc-standards-to-real-world-implementations

This article discusses a specific NIST report that provides guidance on the transition from PQC standards to real world implementations. This focus on practical application is where strategic planning meets execution for businesses.

172. NIST Releases Three Post-Quantum Cryptography Standards | Insights - Holland & Knight

https://www.hklaw.com/en/insights/publications/2024/08/nist-releases-three-post-quantum-cryptography-standards

A major law firm reports on the release of the NIST standards, highlighting the legal and compliance implications. This perspective is crucial for executives in understanding the legal risks of inaction and the need to align with the new standards.

173. Post-Quantum Cryptography - Homeland Security

https://www.dhs.gov/quantum

This is the Department of Homeland Security's official portal for PQC. It outlines the department's strategy and provides resources, signaling the high priority placed on PQC for national and critical infrastructure security.

174. Post-Quantum Cryptography: Sorting Fact from Fiction - AppViewX

https://www.appviewx.com/blogs/post-quantum-cryptography-sorting-fact-from-fiction/

This article aims to clarify common misconceptions about PQC. For leaders, cutting through the noise and understanding the practical realities is essential for making sound strategic decisions.

175. Quantum computing and post-quantum cryptography: what strategy should companies adopt to deal with these issues? - RiskInsight

https://www.riskinsight-wavestone.com/en/2025/03/quantum-computing-and-post-quantum-cryptography-how-to-deal-with-these-issues/

This article directly addresses the question of what corporate strategy should be regarding PQC. It frames the issue in terms of risk management and strategic planning, which is the correct lens for executive leadership.

176. The Post-Quantum Cryptography Migration Starts Today - GovTech

https://www.tech.gov.sg/files/media/Reports/DGX_2024_Cyber_Working_Group_Report.pdf

This report from the Singapore Government's technology agency declares that the PQC migration starts now. It's another strong example of the international consensus and the global nature of the transition.

177. GDIT Joins NIST's Post-Quantum Cryptography Consortium

https://www.gdit.com/about-gdit/press-releases/gdit-joins-nists-post-quantum-cryptography-consortium/

A major Government contractor, GDIT, announces its participation in a NIST consortium. This signals deep industry engagement with the standardization process and a commitment to providing compliant solutions to the public sector.

178. Essential Steps For Post-Quantum Cryptography Readiness - Encryption Consulting

https://www.encryptionconsulting.com/unlocking-the-quantum-era-essential-steps-for-post-quantum-cryptography-readiness/

This article lays out the essential steps for achieving PQC readiness. This type of actionable checklist is valuable for leaders and managers tasked with creating and executing a migration plan.

179. NIST Releases Draft Report on Transition to Post-Quantum Cryptography Standards for Public Comment

https://www.quantum.gov/nist-draft-report-on-pqc-transition/

This announcement covers a draft NIST report on the PQC transition, highlighting the open and collaborative nature of the process. For businesses, this transparency provides opportunities to provide feedback and gain early insight into future requirements.

180. Report on Post-Quantum Cryptography - NIST Technical Series Publications

https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

This is an early (2016) NIST report that helped kick off the PQC standardization process. It provides historical context and shows how long and deliberate the effort to create a quantum safe ecosystem has been.

181. Preparing for Post Quantum Cryptography - Oracle Blogs

https://blogs.oracle.com/security/post/post-quantum-cryptography

Oracle, a massive enterprise software and cloud provider, provides its guidance on preparing for PQC. Their engagement is a critical signal that the core enterprise applications that businesses rely on are being updated to support the new standards.

182. 2024-2025 CRA Quad Paper: The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead - Computing Research Association

https://cra.org/wp-content/uploads/2025/01/2024-2025-CRA-Quad-Paper_-The-Post-Quantum-Cryptography-Transition_-Making-Progress-But-Still-a-Long-Road-Ahead.pdf

This paper from a computing research association provides a balanced academic perspective on the PQC transition. It acknowledges progress while also highlighting the significant challenges that remain, helping executives maintain a realistic view of the e ffort required.

183. 8 Essential Considerations for Post-Quantum Cryptography Migration - AppViewX

https://www.appviewx.com/blogs/8-essential-considerations-for-post-quantum-cryptography-migration/

This article presents a concise list of key considerations for a PQC migration. This type of checklist -based advice is useful for project planning and ensuring all critical aspects of the transition are covered.

184. Overcoming Challenges in the Integration of Post-Quantum Cryptography - Secure-IC

https://www.secure-ic.com/blog/overcoming-challenges-in-the-integration-of-post-quantum-cryptography/

This article focuses on the challenges of integrating PQC, particularly in hardware and embedded systems. It highlights a specific area of complexity that businesses, especially those in manufacturing and IoT, must address.

185. Post-Quantum Computing Security Challenge - AIS Student Chapters - AIS Communities

https://communities.aisnet.org/aisstudentchapters/eventshome/competitions/2025-competitions/postquantumcomputingchallenge

This is an announcement for a student competition focused on PQC security. It signals that the topic is becoming a key part of the academic curriculum, which is crucial for developing the future workforce needed to manage a PQC -enabled world.

186. The quantum threat: Addressing challenges in post-quantum cryptography - Outshift | Cisco

https://outshift.cisco.com/blog/post-quantum-cryptography-addressing-challenges

Cisco, a dominant force in networking hardware, discusses the challenges of PQC. Their focus on the issue is critical, as the transition will heavily rely on network infrastructure being updated to support the new standards.

187. Mitigating Quantum Threats Beyond Post-Quantum Cryptography (PQC) - Marin Ivezic

https://postquantum.com/post-quantum/mitigating-quantum-threats-pqc/

This article explores security strategies that go beyond just swapping algorithms. It encourages a defense in depth approach, which is a key principle of modern cybersecurity that should be applied to the quantum threat as well.

188. Cyber officials cite legacy systems as post -quantum readiness challenge - FedScoop

https://fedscoop.com/cyber-officials-cite-legacy-systems-as-post-quantum-readiness-challenge/

This news report highlights legacy systems as a major roadblock to the Federal PQC transition. This is a critical risk factor that all large organizations must address, as these older systems are often the hardest and most expensive to upgrade.

189. The Looming Quantum Migration: Why Cryptography Inventory is Essential - Utimaco

https://utimaco.com/news/blog-posts/looming-quantum-migration-why-cryptography-inventory-essential

This article stresses the absolute necessity of conducting a comprehensive cryptographic inventory. For executives, this is the non- negotiable first step; you cannot protect what you do not know you have.

190. Post Quantum Cryptography Training in United States of America - Bilginç IT Academy

https://bilginc.com/us/training/post-quantum-cryptography-6792-training/

This is an advertisement for PQC training, indicating the emergence of a commercial training market to address the skills gap. Investing in workforce development will be a critical success factor for any business's PQC migration.

191. Best Quantum Cryptography Courses & Certificates [2025] | Coursera Learn Online

https://www.coursera.org/courses?query=quantum%20cryptography

This page lists online courses available for quantum cryptography. The availability of courses on major platforms like Coursera makes PQC knowledge more accessible, helping businesses improve their existing workforce to meet the new challenges.

192. What are the Implications of Post-Quantum Computing on Security and Cryptography?

https://www.schellman.com/blog/cybersecurity/implications-of-post-quantum-computing-on-security-and-cryptography

This article from a compliance and attestation firm explores the implications of PQC for security audits. It signals that PQC readiness will soon become a standard item on compliance checklists like SOC 2 and ISO 27001.

193. Evaluation Framework for Quantum Security Risk Assessment - arXiv

https://arxiv.org/pdf/2404.08231

This academic paper proposes a formal framework for assessing quantum security risks. As this research matures, it will provide businesses with more rigorous and standardized methods for quantifying their quantum risk exposure.

194. Key Post-Quantum Cryptography Insights from the Executive Order On Strengthening And Promoting Innovation in the Nation's Cybersecurity -AppViewX

https://www.appviewx.com/blogs/key-post-quantum-cryptography-insights-from-the-executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/

This article breaks down the PQC -related implications of a White House Executive Order. This type of analysis helps businesses understand the specific compliance requirements and strategic shifts being driven by Federal policy.

195. Preparing for Post-Quantum Cryptography - Apriorit

https://www.apriorit.com/dev-blog/prepare-for-post-quantum-cryptography-with-crypto-agility

This article links the preparation for PQC directly to the concept of crypto agility. The key message for leaders is that the goal is not just to implement the new standards, but to build systems that can adapt to future cryptographic transitions easily.

196. How Quantum Computing Will Impact the Defense Sector - Cevians

https://www.cevians.com/how-quantum-computing-will-impact-the-defense-sector/

This article focuses specifically on the impact of quantum computing on the defense sector. The long lifespan of military systems and the high value of classified data make this sector a critical area for immediate PQC adoption.

197. Inside the Quantum-Powered Defense Landscape of the Future - GovCon Wire

https://www.govconwire.com/2025/01/future-quantum-defense-applications/

This piece looks at the future applications of quantum technology in defense, beyond just code -breaking. For defense contractors, understanding this broader landscape is key to aligning their R&D and business strategies with future customer needs.

198. The Integration of Quantum Computing in Military Applications - Defence Industries

https://www.defence-industries.com/articles/the-integration-of-quantum-computing-in-military-applications

This article discusses the integration of quantum computing into military applications. It reinforces the dual nature of the technology as both a threat that must be defended against with PQC and a capability that offers new strategic advantages.

199. Helping a Major Intelligence Agency Become Quantum-Ready - GDIT

https://www.gdit.com/perspectives/client-stories/helping-a-major-intelligence-agency-become-quantum-ready/

This case study from a major contractor details their work in helping an intelligence agency prepare for the quantum threat. It provides a real world example of the scale and complexity of PQC migration in a high -security environment.

200. Intelligence After Next: Quantum Computing–Quantifying the Current State of the Art to Assess Cybersecurity Threats | MITRE

https://www.mitre.org/news-insights/publication/intelligence-after-next-quantum-computing-quantifying-current-state-art

This report from MITRE, a federally funded research center, provides a detailed assessment of the quantum threat from an intelligence perspective. This type of in depth analysis from a trusted source is crucial for informing national security policy and strategy.

201. Quantum Computing: What Agencies Need to Know - GDIT

https://www.gdit.com/perspectives/latest/quantum-computing-what-agencies-need-to-know/

This article provides a high level overview of quantum computing tailored for Federal agency leaders. It is a good example of the educational material that contractors are providing to help their Government customers understand and address the quantum threat.

202. GDIT Study Shows Federal IT's Efforts to Adopt Post -Quantum Cryptography

https://washingtonexec.com/2024/10/gdit-report-federal-it-accelerating-post-quantum-cryptography-strategies/

This report highlights the progress and challenges of PQC adoption within Federal IT. For executives, this type of on -the ground data is valuable for benchmarking their own organization's progress against the broader public sector.

203. Quantum Computing and Homeland Security: Preparing for a New Age of Cyber Defense

https://www.juvare.com/quantum-computing-and-homeland-security-preparing-for-a-new-age-of-cyber-defense/

This article focuses on the specific implications of quantum computing for homeland security. It covers critical infrastructure protection and other key DHS mission areas where PQC is becoming a critical requirement.

204. Quantum Computing and the Future of Cybersecurity - The National CIO Review

https://nationalcioreview.com/articles-insights/information-security/quantum-computing-and-the-future-of-cybersecurity/

This article provides a strategic overview of quantum computing's impact on cybersecurity from a CIO's perspective. It frames the issue in terms of enterprise wide risk management, IT strategy, and governance.

205. Quantum AI in Cybersecurity – Revolutionizing Defense Mechanisms and Threat Landscapes – cyber enterprise solutions

https://www.cyberenterprisesolutions.com/quantum-ai-in-cybersecurity-revolutionizing-defense-mechanisms-and-threat-landscapes/

This article explores the intersection of quantum computing and artificial intelligence in cybersecurity. For leaders, it is crucial to understand that these two disruptive technologies will evolve together, creating both new threats and new defensive capabilities.

206. The Relationship Between AI and Quantum Computing | CSA - Cloud Security Alliance

https://cloudsecurityalliance.org/blog/2025/01/20/quantum-artificial-intelligence-exploring-the-relationship-between-ai-and-quantum-computing

The Cloud Security Alliance discusses the relationship between AI and quantum computing. This highlights the importance for businesses, particularly those heavily invested in the cloud, to have a strategy that accounts for the convergence of these two powerful technologies.

207. The End of RSA and ECC? How PUF- Based PQC is Redefining Cybersecurity -1950.ai

https://www.1950.ai/post/the-end-of-rsa-and-ecc-how-puf-based-pqc-is-redefining-cybersecurity

This article declares the effective "end" of RSA and ECC and explores novel hardware- based approaches to PQC. While NIST standards are software focused, executives should be aware of emerging hardware solutions that could play a role in a long term security strategy.

208. The Quantum Man and the Sea of Risks - CSIS

https://www.csis.org/analysis/quantum-man-and-sea-risks

This analysis from the Center for Strategic and International Studies (CSIS) uses an analogy to explain the vast and complex landscape of quantum risks. This type of strategic brief from a major think tank is essential for framing the issue in a geopoliti cal and national security context.

209. The government unveils its quantum counter-weapons - POLITICO

https://www.politico.com/newsletters/digital-future-daily/2024/08/13/the-government-unveils-its-quantum-counter-weapons-00173832

This POLITICO article reports on the Government's PQC strategy in accessible, policy - focused language. This type of mainstream coverage is a key indicator that PQC has moved from a technical issue to a major public policy concern.

210. Governments must prepare for quantum computing risks

https://www.openaccessgovernment.org/governments-must-prepare-for-quantum-computing-risks/181886/

This article argues for the necessity of Government preparation for quantum risks. For businesses that work with the public sector, this reinforces the idea that PQC readiness will increasingly become a mandatory requirement for Government contracts.

211. Post- Quantum Cryptography (PQC) Meets Quantum Artificial Intelligence (QAI) - Marin Ivezic

https://postquantum.com/post-quantum/post-quantum-cryptography-pqc-meets-quantum-artificial-intelligence-qai/

This article explores the convergence of PQC and quantum AI. The key insight for executives is that the future of cybersecurity will be a dynamic interplay between quantum attacks (potentially enhanced by AI) and quantum defenses (also enhanced by AI).

212. The Impact Of AI On Post-Quantum Cybersecurity - Forbes

https://www.forbes.com/councils/forbestechcouncil/2024/02/06/the-impact-of-ai-on-post-quantum-cybersecurity/

This Forbes article delves into how AI will impact the PQC transition. AI can be used to accelerate the discovery of cryptographic assets and the testing of new PQC implementations, making it a critical enabling technology for migration.

213. 2025 Expert Quantum Predictions -- PQC And Quantum Cybersecurity

https://thequantuminsider.com/2024/12/31/2025-expert-quantum-predictions-pqc-and-quantum-cybersecurity/

This article aggregates expert predictions for PQC in the coming year. Such forecasts are valuable for business leaders to anticipate near- term trends and adjust their strategic plans accordingly.

214. The New Federal Quantum Action Plan | Encryption Consulting

https://www.encryptionconsulting.com/your-guide-to-the-new-federal-quantum-action-plan/

This article provides a guide to the Federal Government's action plan for PQC. Understanding this plan is essential for any business that operates in the public sector or is part of a critical infrastructure industry.

215. Quantum Computing, Artificial Intelligence, and the Cybersecurity ...

https://www.accessitgroup.com/quantum-computing-artificial-intelligence-and-the-cybersecurity-threat-landscape/

This piece provides another look at the intersection of AI, quantum computing, and cybersecurity. The recurring theme across multiple sources highlights the importance for executives to have an integrated strategy that addresses all three domains.

216. Quantum Computing and Cybersecurity – Preparing for a New Age of Threats | MSSP Alert

https://www.msspalert.com/native/quantum-computing-and-cybersecurity-preparing-for-a-new-age-of-threats

This article, aimed at Managed Security Service Providers (MSSPs), signals that PQC is becoming a new service line and competency for the outsourced security market. This means businesses will soon be able to procure PQC expertise and management as a service.

217. Quantum Threat Mitigation - Merlin Cyber

https://www.merlincyber.com/quantum-threat-mitigation

This solution brief from a cybersecurity vendor outlines their approach to mitigating the quantum threat. It's an example of the commercially available tools and services that businesses can leverage to support their PQC transition.

218. CISA Details PQC Migration Roadmap, Plans to Release 'Very Soon' -MeriTalk

https://www.meritalk.com/articles/cisa-details-pqc-migration-roadmap-plans-to-release-very-soon/

This news report announced CISA's forthcoming PQC migration roadmap. CISA delivered on that commitment in January 2026 with the Product Categories for Technologies That Use Post Quantum Cryptography Standards, cited later in this index, giving businesses the clear, Government backed framework the article anticipated.

219. CISA: 2035 Quantum Encryption Deadline Still Achievable - Bank Info Security

https://www.bankinfosecurity.com/cisa-2035-quantum-encryption-deadline-still-achievable-a-27110

This article reports CISA's assessment that the Government's PQC transition deadline is achievable. This message of confidence from a key Federal agency can help reassure business leaders that migration, while challenging, is a manageable endeavor.

220. President Biden Issues Last-Minute Cybersecurity Executive Order

https://www.hunton.com/privacy-and-information-security-law/president-biden-issues-last-minute-cybersecurity-executive-order

This legal analysis covers a White House cybersecurity Executive Order. These high level directives are the primary drivers of Federal cybersecurity policy and create cascading compliance requirements for the private sector.

221. FACT SHEET: New Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity | The White House - Joe Biden for President

https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/15/fact-sheet-new-executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/

This is an official White House fact sheet explaining a new cybersecurity Executive Order. It is a primary source document that businesses must consult to understand their compliance obligations and the strategic direction of Federal policy.

222. Executive Order 14144: What OT-ICS Leaders Need to Know | Verve Industrial

https://verveindustrial.com/resources/blog/executive-order-14144-ot-ics/

This article analyzes Executive Order 14144 from the perspective of industrial control system operators. It highlights the critical need for businesses in the OT space to pay close attention to PQC mandates, as their systems are often the most challenging to upgrade.

223. A New Dawn in Cyber Defense: Understanding Executive Order 14144 | Fortanix

https://www.fortanix.com/blog/a-new-dawn-in-cyber-defense-understanding-executive-order-14144

This article provides an analysis of a cybersecurity Executive Order from a vendor's perspective. It helps businesses translate the high- level policy of an EO into specific technical capabilities and solutions.

224. Biden Expands Cybersecurity Mandate, Targets AI and Quantum Risks

https://thequantuminsider.com/2025/01/17/biden-expands-cybersecurity-mandate-targets-ai-and-quantum-risks/

This news report highlights the expansion of Federal cybersecurity mandates to explicitly include AI and quantum risks. This is a critical development for executives, as it officially places PQC readiness on the list of top -level Federal compliance priorities.

225. EXECUTIVE ORDER 14144 - - - - - STRENGTHENING AND PROMOTING INNOVATION IN THE NATION'S CYBERSECURITY By the authority vested -Federal Register

https://public-inspection.federalregister.gov/2025-01470.pdf

This is the official publication of Executive Order 14144, signed January 16, 2025, in the Federal Register. Publication in the Federal Register is the formal step that gives EOs and other regulations the force of law, and the order was subsequently amended by Executive Order 14306 in June 2025.

226. Demystifying the Connection Between Quantum Computing & Encryption - Portal26

https://portal26.ai/demystifying-the-connection-between-quantum-computing-and-encryption/

This article aims to simplify the relationship between quantum computing and encryption for a business audience. Clear, accessible explanations are key to building broad organizational understanding and support for the PQC migration.

227. Shor's Factorization Algorithm - GeeksforGeeks

https://www.geeksforgeeks.org/shors-factorization-algorithm/

This is a more technical, developer focused explanation of Shor's algorithm. While aimed at programmers, it provides detailed evidence that technical teams need to support the business case for PQC presented to leadership.

228. Shor's Factoring Algorithm (for Dummies) Step-by-Step with example - Kaustubh Rakhade

https://kaustubhrakhade.medium.com/shors-factoring-algorithm-94a0796a13b1

This article provides a simplified, step -by step guide to Shor's algorithm. This type of accessible explanation is useful for educating non technical stakeholders on the mechanics of the quantum threat.

229. Addressing the Quantum Threat in the US Federal Government | Ping Identity

https://www.pingidentity.com/en/resources/blog/post/quantum-threat-us-fed-gov.html

An identity management company addresses the quantum threat in the Federal Government. This highlights the critical impact of PQC on identity and authentication systems, a cornerstone of Zero Trust architecture.

230. Protecting Your Federal Benefits from Quantum Threats

https://stwserve.com/protecting-your-federal-benefits-from-quantum-threats/

This article targets a specific audience, Federal employees, to explain the quantum threat to their benefits. This illustrates how the PQC issue has broad implications, extending to the security of personally identifiable information (PII) for millions of c itizens.

231. Cybersecurity Analysis: Implications of quantum computing on encryption and legal frameworks - Steele Fortress

https://steelefortress.com/fortress-feed/cybersecurity-analysis-implications-of-quantum-computing-on-encryption-and-legal-frameworks

This analysis covers both the technical and legal implications of quantum computing. For executives, this is a crucial link, as the technical transition to PQC must be managed in parallel with evolving legal and compliance frameworks.

232. Post-Quantum Cryptography - Qujata

https://www.qujata.com/national-security

This is a solution page from a PQC vendor focusing on the national security sector. It's an example of specialized commercial solutions that are emerging to meet the specific needs of the defense and intelligence communities.

233. Why we must quantum-proof our critical infrastructure | Smart Energy ...

https://www.smart-energy.com/industry-sectors/digitalisation/why-we-must-quantum-proof-our-critical-infrastructure/

This article argues for the necessity of "quantum- proofing" critical infrastructure in the energy sector. It highlights the extreme vulnerability of industrial control systems and the potentially catastrophic consequences of a quantum attack.

234. Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy - GAO

https://www.gao.gov/products/gao-25-107703

This is the main product page for the GAO report on the quantum threat. The report's key findings for executives are its call for centralized leadership and a clear, actionable strategy, a gap that businesses must also address in their own internal planning.

235. H.R.5759 - 118th Congress (2023-2024): Post Quantum Cybersecurity Standards Act

https://www.congress.gov/bill/118th-congress/house-bill/5759/history

This is a link to a real (though not enacted) bill related to PQC standards. It demonstrates that Congress is actively considering legislation to mandate and standardize the PQC transition, adding to the regulatory pressure on both Government and industry.

236. How Will the Trump Administration Handle Quantum Policy? | GovCIO Media & Research

https://govciomedia.com/how-will-the-trump-administration-handle-quantum-policy/

This article speculates on the future of quantum policy under a different administration. For business strategy, it highlights that while the specific approach may change, the underlying national security imperative to address the quantum threat will remain, regardless of the political party in power.

237. Client Alert: White House Executive Order Seeks to Strengthen Federal Cybersecurity

https://www.jenner.com/en/news-insights/publications/client-alert-white-house-executive-order-seeks-to-strengthen-federal-cybersecurity

This is a client alert from a law firm analyzing a White House cybersecurity Executive Order. These alerts are a keyway for businesses to receive expert legal interpretation of new Government mandates and understand their specific compliance obligations.

238. NIST approves three quantum-resistant encryption standards, bolsters cybersecurity posture

https://industrialcyber.co/nist/nist-approves-three-quantum-resistant-encryption-standards-bolsters-cybersecurity-posture/

This article reports on the final approval of the first NIST PQC standards. The finalization of these standards is the single most important trigger for businesses, as it removes uncertainty and provides a clear, stable target for migration.

239. NIST Releases Post-Quantum Encryption Standards

https://www.quantum.gov/nist-releases-post-quantum-encryption-standards/

This is an official announcement from the National Quantum Initiative on the release of the NIST standards. It is a primary source document that marks the formal beginning of the operational phase of the U.S. national PQC transition.

240. What is Quantum Computing? [Everything You Need to Know]

https://thequantuminsider.com/2024/02/02/what-is-quantum-computing/

This guide provides a comprehensive but accessible overview of quantum computing. It is a good foundational resource for executives and teams who are new to the topic.

241. What is Quantum Computing? - AWS

https://aws.amazon.com/what-is/quantum-computing/

Amazon Web Services explains quantum computing. As the largest cloud provider, their focus on and investment in this technology is a critical market signal that quantum capabilities and quantum safe security will be major components of the future cloud ec osystem.

242. Quantum Computing Basics: A Beginner's Guide - BlueQubit

https://www.bluequbit.io/quantum-computing-basics

This is another introductory guide to the basics of quantum computing. The availability of multiple such guides from various companies indicates a strong market focus on educating potential customers about technology.

243. Physical Principles Underpinning Quantum Computing - EE Times Europe

https://www.eetimes.eu/physical-principles-underpinning-quantum-computing/

This article delves into the underlying physics of quantum computing. While technical, a high level understanding helps leaders appreciate the profound difference in how these machines operate and why they pose such a unique threat.

244. Shor's Algorithm: A Quantum Threat to Modern Cryptography

https://postquantum.com/post-quantum/shors-algorithm-a-quantum-threat/

This article positions Shor's algorithm as the central threat to modern cryptography. This problem- centric framing is useful for justifying the business need for a solution (PQC).

245. Quantum Computing: Implications for Security Professionals - TrueFort

https://truefort.com/quantum-computing-security/

This article focuses on the implications of quantum computing for the security profession. It highlights the need for upskilling and a new way of thinking about cryptographic risk management.

246. NIST Quantum Standards: Security Experts Talk Hurdles | Cyber Magazine

https://cybermagazine.com/articles/race-to-shield-data-from-tomorrows-quantum-code-breakers

This article gathers expert opinions on the challenges of implementing the new NIST PQC standards. Understanding these practical hurdles is crucial for executives to develop a realistic migration plan and budget.

247. GAO Warns of Quantum Threat to U.S. Cybersecurity Amid Leadership and Strategy Gaps

https://thequantuminsider.com/2024/11/22/gao-warns-of-quantum-threat-to-u-s-cybersecurity-amid-leadership-and-strategy-gaps/

This news report covers the GAO's warning about a lack of leadership in the Federal PQC effort. This external validation of the strategic gap puts pressure on both Government and industry leaders to step up and take ownership of the transition.

248. GAO-25- 107703, Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy

https://www.gao.gov/assets/gao-25-107703.pdf

This is a direct link to the full PDF of the GAO report. This primary source document is the definitive authority for understanding the GAO's findings and recommendations, and it should be a key document in any business's PQC strategy library.

249. Quantum-Safe Critical Infrastructure Protection

https://qubridge.io/quantum-safe-critical-infrastructure-protection/

This solution brief focuses on PQC for critical infrastructure protection. It's an example of the specialized, sector- specific solutions that are emerging to address the unique challenges of industries like energy, water, and transportation.

250. Quantum-safe networks | Nokia.com

https://www.nokia.com/industries/quantum-safe-networks/

Nokia, a major telecommunications equipment provider, outlines its approach to quantum safe networks. Their commitment is a crucial signal that the core infrastructure of global communications is being upgraded to support PQC.

251. Quantum Computing Cybersecurity Preparedness Act - PostQuantum.com

https://postquantum.com/industry-news/quantum-preparedness-act/

This article explains the significance of the Quantum Computing Cybersecurity Preparedness Act. Understanding this legislation is key for any business that works with the U.S. Government.

252. What The Quantum Computing Cybersecurity Preparedness Act Means For National Security - Forbes

https://www.forbes.com/councils/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/

This Forbes article analyzes the national security implications of the PQC Preparedness Act. It connects the legal requirements of the act directly to the broader strategic imperative to protect the nation from quantum threats.

253. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House

https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

This is the official White House page for NSM-10, the foundational policy document for the U.S. Government's PQC strategy. It is the primary source for understanding the executive branch's goals and directives on this topic.

254. H.R.7535 - 117th Congress (2021 -2022): Quantum Computing Cybersecurity Preparedness Act

https://www.congress.gov/bill/117th-congress/house-bill/7535

This is the official Congress.gov page for the PQC Preparedness Act. This primary source provides the exact text of the law, which is essential for legal and compliance teams to determine their organization's obligations.

255. Quantum Computing: Examining the Quantum Computing Cybersecurity Preparedness Act | Insights | Holland & Knight

https://www.hklaw.com/en/insights/publications/2023/01/quantum-computing-examining-the-quantum-computing-cybersecurity

A law firm examines the PQC Preparedness Act, providing legal analysis and interpretation. This type of expert commentary is valuable for business leaders in understanding the practical compliance implications of the law.

256. NIST Releases First 3 Finalized Post -Quantum Encryption Standards

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

This is the official press release from NIST announcing the finalization of the first PQC standards. This announcement marks the official start of the implementation phase of the global PQC transition.

257. Workshops and Timeline - Post-Quantum Cryptography | CSRC

https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

This NIST page provides a timeline and history of the workshops that led to the PQC standards. It showcases the open, collaborative, and international nature of the standardization process, which builds confidence in the final results.

258. US unveils new tools to withstand encryption-breaking quantum | World Economic Forum

https://www.weforum.org/stories/2024/08/us-tools-encryption-breaking-quantum-computing-nist/

The World Economic Forum reports on the release of the NIST standards, framing it as a major development in the global effort to counter quantum threats. This high -level international perspective underscores the global significance of the PQC transition.

259. Tackling the Quantum Threat: Applying NIST's Standards Globally - Infosecurity Europe

https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/quantum-threat-nist-standards.html

This article discusses the global application of the NIST standards. For multinational corporations, this highlights the likelihood that the NIST standards will become the de facto global benchmark for PQC.

260. NIST Roadmap to Post- Quantum Cryptography: IR 8547 Report - InfoSec Global

https://www.infosecglobal.com/posts/nist-post-quantum-cryptography-deadlines-ir-8547

This article analyzes a specific NIST report that provides a roadmap and deadlines for the PQC transition. Such roadmaps are critical for business planning, as they provide clear milestones and timelines to which internal plans can be aligned.

261. CISA: How post-quantum cryptography safeguards against quantum threats

https://www.innovationnewsnetwork.com/cisa-how-post-quantum-cryptography-safeguards-against-quantum-threats/54045/

This article provides CISA's perspective on how PQC provides protection against quantum threats. As the lead civilian cybersecurity agency, CISA's endorsement and guidance are critical drivers for PQC adoption in the private sector, especially in critical infrastructure.

262. Post-Quantum Cryptography: Preparing for the Future of Security - Auth0

https://auth0.com/blog/post-quantum-cryptography/

An identity and access management company discusses preparing for PQC. This highlights the critical impact of the PQC transition on authentication and digital identity, a core component of modern enterprise security.

263. Exploring Elliptic Curve vs. Lattice-Based Cryptography for Future Security - Medium

https://medium.com/@RocketMeUpCybersecurity/exploring-elliptic-curve-vs-lattice-based-cryptography-for-future-security-0c8426c97deb

This article compares the old cryptographic standard (ECC) with the new one (lattice- based PQC). This helps business leaders understand that the transition is not just an upgrade but a fundamental shift to a new mathematical foundation for security.

264. Lattice-Based Cryptography - ISARA Corporation

https://www.isara.com/blog-posts/lattice-based-cryptography.html

A PQC vendor explains lattice based cryptography. The availability of clear explanations from multiple commercial sources shows a market that is mature enough to educate its customers on the underlying technology.

265. The Weaknesses of Post-quantum Cryptography - Quantropi

https://www.quantropi.com/3-weaknesses-of-post-quantum-cryptography/

This article discusses potential weaknesses or challenges of PQC, such as performance overhead. It is crucial for business leaders to understand these potential downsides to make informed decisions and plan for any necessary infrastructure upgrades.

266. What Is Hash-Based Cryptography? Quantum-Resilient Algorithm »

https://www.quantumize.com/what-is-hash-based-cryptography/

This article provides a specific explanation of hash -based cryptography as a quantum-resilient solution. Understanding this specific type of PQC helps businesses appreciate the value of algorithmic diversity in their security portfolio.

267. Is Hashing Secure Than Encryption

https://www.encryptionconsulting.com/education-center/encryption-vs-hashing/

This article compares the security properties of hashing and encryption. This distinction is important in the PQC context, as hashing is a core component of some of the most secure PQC signature schemes.

268. (PDF) Critical attacks in code-based cryptography - ResearchGate

https://www.researchgate.net/publication/281657709_Critical_attacks_in_code-based_cryptography

This academic paper discusses potential attacks on code based cryptography. The ongoing research into both the strengths and weaknesses of PQC algorithms is a sign of a healthy and mature research community, which ultimately leads to stronger standards.

269. Code-based Cryptography

https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_simona-samardjiska_radboud-university_code-based-cryptography.pdf

This is a presentation from a conference on code based cryptography. It provides insight into the academic and research community that is working to ensure the long term security and viability of this PQC approach.

270. Math Paths to Quantum-Safe Security: Isogeny-Based Cryptography - ISARA Corporation

https://www.isara.com/blog-posts/isogeny-based-cryptography.html

This article explains the mathematical principles of isogeny based cryptography. It's another example of deep research that has gone into exploring different pathways to quantum -safe security.

271. Review of Chosen Isogeny-Based Cryptographic Schemes - MDPI

https://www.mdpi.com/2410-387X/6/2/27

This academic paper reviews various isogeny based cryptographic schemes. The rigorous academic review process is a critical part of vetting and building confidence in new cryptographic standards.

272. A Study on Isogeny Based Cryptography - Inspire HEP

https://inspirehep.net/literature/2815279

This is another academic study on isogeny based cryptography. The breadth of research in this area, even though it did not produce a final NIST standard, shows the thoroughness of the search for quantum resistant algorithms.

273. Complete Analysis of Implementing Isogeny- based Cryptography using Huff Form of Elliptic Curves - Cryptology ePrint Archive

https://eprint.iacr.org/2021/085.pdf

This highly technical paper provides a detailed analysis of implementing a specific type of isogeny -based cryptography. This level of detail is representative of the deep research required to bring new cryptographic concepts to maturity.

274. Post-quantum Cryptography: Maybe We Should Just Use Symmetric Keys

https://twosixtech.com/blog/post-quantum-cryptography-maybe-we-should-just-use-symmetric-keys/

This article explores an alternative approach to PQC, focusing on architectures that rely more heavily on symmetric -key cryptography, which is less vulnerable to quantum attacks. This highlights that the PQC transition may involve architectural changes, not just algorithm swaps.

275. Symmetric key cryptography - IBM Quantum Learning

https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/symmetric-key-cryptography

This IBM course module explains symmetric key cryptography in the context of PQC. The key takeaway is that symmetric algorithms like AES remain a core part of a quantum safe strategy, provided that sufficiently long keys are used.

SECTION 16

Crypto Agility

276. Cryptographic agility in the zeitgeist | CMS Information Security & Privacy Group

https://security.cms.gov/posts/cryptographic-agility-zeitgeist

This article from a Federal agency group highlights the growing importance of crypto agility. It signals that the Government sees the PQC transition not as a final step, but as one of many future cryptographic migrations that systems must be prepared for.

277. Crypto agility in the Post-quantum Era: The Key to the IT Security of the Future - InfoGuard

https://www.infoguard.ch/en/blog/crypto-agility-in-post-quantum-era-the-key-to-it-security-of-future

This article positions crypto agility as a key to future IT security. The core business insight is that building agile systems now will significantly reduce the cost and disruption of all future cryptographic transitions.

278. NIST CSWP 39, Considerations for Achieving Crypto Agility: Strategies and Practices (Final)

https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/final

This finalized NIST publication provides the standard framework and best practices for building systems that can swap cryptographic algorithms without redesign. OMB Memorandum M-26-15 cites it directly in its implementation guidance, which makes crypto agility a reference architecture behind a Federal mandate rather than a best practice argument.

279. Crypto-agility: Preparing for post-quantum decryption - Accenture

https://www.accenture.com/us-en/insightsnew/us-federal-government/post-quantum-cryptography

Accenture, a major global consultancy, emphasizes crypto- agility as a core component of PQC preparation. Their focus on this topic indicates that it has become a key strategic recommendation for enterprises undertaking the PQC transition.

280. Introduction to Crypto-Agility - PostQuantum.com

https://postquantum.com/post-quantum/introduction-crypto-agility/

This article provides a clear introduction to the concept of crypto agility. For executives, this is a crucial concept to grasp: the goal is not just to migrate to PQC, but to build systems that are no longer dependent on a single, hard -coded cryptographic algorithm.

281. Feds: Crypto-Agility Looms Larger Than Post-Quantum Crypto - MeriTalk

https://www.meritalk.com/articles/feds-crypto-agility-looms-larger-than-post-quantum-crypto/

This news report suggests that for Federal agencies, the long term goal of achieving crypto agility is even more important than the immediate task of migrating to PQC. This strategic perspective should inform business planning, focusing on building for th e future, not just solving today's problem.

282. Embracing Crypto-agility for Quantum-safe Business - Tata Consultancy Services

https://www.tcs.com/what-we-do/services/cybersecurity/white-paper/crypto-agility-quantum-computing-safety

This white paper from a major IT services firm makes the business case for crypto -agility as part of a quantum safe strategy. It provides a roadmap for how businesses can implement agile practices to reduce long term security risk and cost.

283. Case Study Details - The Quantum Economy Network - Real World Cryptographic Agility

https://initiatives.weforum.org/quantum/case-study-details/real-world-cryptographic-agility/aJYTG0000000KWb4AM

This case study from the World Economic Forum showcases a real world example of cryptographic agility. These practical examples are invaluable for business leaders to understand how the concept can be translated into a successful implementation.

284. NIST Outlines Strategies for Crypto Agility as PQC Migration Stalls, Available for Public Comment - The Quantum Insider

https://thequantuminsider.com/2025/03/07/nist-outlines-strategies-for-crypto-agility-as-pqc-migration-stalls-available-for-public-comment/

This article reports on new NIST guidance for crypto agility. It underscores that the Government is actively pushing for agility as a core principle of modern cybersecurity, adding weight to the business case for investing in it.

SECTION 17

Historical Transitions and Military Applications

285. How to Transition from DES to Advanced Encryption Standard (AES) - Blogs

https://blogs.eshare.ai/how-to-transition-from-des-to-advanced-encryption-standard-aes/

This article looks back at the historical migration from the DES to the AES encryption standard. This precedent is a useful case study for businesses planning their PQC transition, offering lessons learned from a previous, large scale cryptographic migration.

286. Transition to Advanced Encryption Standard (AES) - CISA

https://www.cisa.gov/sites/default/files/2024-05/23_0918_fpic_AES-Transition-WhitePaper_Final_508C_24_0513.pdf

This official CISA document details the transition to AES. It provides a Government backed example of a successful cryptographic modernization effort and the kind of planning and coordination required.

287. The transition to advanced encryption standard - U.S. Fire Administration - FEMA

https://www.usfa.fema.gov/blog/the-transition-to-advanced-encryption-standard/

This blog post from a specific Federal agency discusses the AES transition. It illustrates how cryptographic migrations impact all corners of the Government and the importance of sector-specific planning.

288. Quantum Technology in the Military - NSTXL

https://nstxl.org/quantum-technology-in-the-military/

This article focuses on the military applications of quantum technology. For the defense industry, understanding these applications is key to aligning products and services with the future needs of their primary customers.

289. Quantum's Role in the Intelligence Community - GovLoop

https://www.govloop.com/community/blog/quantums-role-in-the-intelligence-community/

This article explores the role of quantum technology within the Intelligence Community. The high stakes nature of intelligence work makes this sector a key driver for the adoption of the most secure PQC and QKD solutions.

290. MITRE Paper Discusses Role of IC in Quantum Computing Race - ExecutiveGov

https://executivegov.com/2025/01/mitre-intelligence-community-quantum-computing/

This report covers a MITRE paper on the Intelligence Community's role in the quantum race. It highlights the dual role the IC plays in both defending against foreign quantum threats and developing its own quantum capabilities.

291. Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy - Government Accountability Office (GAO)

https://www.gao.gov/products/gao-25-107703

This is the official page for the key GAO report on quantum readiness. The report's central conclusion, that a lack of centralized leadership is hampering the national response, is a critical finding for both policymakers and the businesses that support the m.

292. M-23-02, Memorandum for Heads of Executive Departments and Agencies: Migrating to Post-Quantum Cryptography

https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

This is the official OMB memorandum that put the requirements of NSM-10 into action for Federal agencies, defining the original requirements for cryptographic inventories and migration planning. OMB Memorandum M-26-15, issued in June 2026 and cited later in this index, now carries the operative migration guidance, and the inventories built under M-23-02 feed directly into its first phase.

293. H.R.7535 - Quantum Computing Cybersecurity Preparedness Act

https://www.congress.gov/bill/117th-congress/house-bill/7535

This is the official congressional page for the PQC Preparedness Act. This law provides legislative backing for the executive branch's PQC mandates.

294. NIST Releases First Three Finalized Post -Quantum Encryption Standards

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

This official NIST press release marks the most significant milestone in the PQC transition. The finalization of the standards provides a stable, long- term technical target for all PQC implementations.

295. Announcing the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

This is the official NSA announcement for CNSA 2.0, which specifies the PQC algorithms required for National Security Systems. This document is the primary driver for PQC adoption in the defense and intelligence sectors.

296. Post-Quantum Considerations for Operational Technology

https://www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology

This is the official CISA page for its guidance on PQC in OT environments. It is an essential read for any business operating critical infrastructure.

297. Project Leap: Leaping to quantum-safe payments

https://www.bis.org/publ/othp79.htm

This is the official page for the Bank for International Settlements' "Project Leap." It is a key case study demonstrating that the global financial system is actively preparing for the PQC transition.

298. NTT introduces world's first commercially available post -quantum cryptography system

https://group.ntt/en/newsrelease/2024/10/24/241024a.html

This is the official press release from NTT about their commercial PQC system. It marks a key milestone in the maturation of the PQC market from research to commercially available products.

299. Europol's Quantum-Safe Financial Forum - A call to action

https://www.europol.europa.eu/media-press/newsroom/news/europols-quantum-safe-financial-forum-call-to-action

This official announcement from Europol underscores the international law enforcement consensus on the need for the financial sector to migrate to PQC. This adds regulatory and security pressure on financial institutions worldwide.

300. Announcing quantum-safe digital signatures in Cloud KMS

https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-digital-signatures-in-cloud-kms

This is the official Google Cloud blog post announcing the availability of PQC in their Key Management Service. This is a major market development, as it makes PQC capabilities easily accessible to the millions of customers using their cloud platform.

301. ENISA Space Threat Landscape 2025

https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025

This is the official page for the European Union Agency for Cybersecurity's report on space threats. The inclusion of quantum as a major threat highlights the critical need for PQC in the satellite and aerospace industries.

302. How to factor 2048 bit RSA integers with less than a million noisy qubits

https://arxiv.org/abs/2505.15917

In this May 2025 paper, Craig Gidney of Google Quantum AI cuts his own 2019 estimate of 20 million noisy qubits for factoring RSA-2048 down to under one million, with a runtime under a week. Research like this continuously shortens the projected timeline for a CRQC, increasing the urgency for businesses to complete their PQC migration.

303. China Quantum Chip — Zuchongzhi 3.0 — Claims Google's QA Benchmark Title

https://www.hpcwire.com/2025/03/04/china-quantum-chip-zuchongzhi-3-0-claims-googles-qa-benchmark-title/

This news article reports on a significant hardware advance by a strategic competitor. Such developments are key geopolitical drivers for the U.S. Government's accelerated PQC timelines and should be monitored closely by businesses in the defense sector.

304. China Telecom Launches Hybrid Quantum-Safe Encryption System, Completes 1,000-Kilometer Secure Call

https://thequantuminsider.com/2025/05/20/china-telecom-launches-hybrid-quantum-safe-encryption-system-completes-1000-kilometer-secure-call/

This report on a large scale deployment of quantum safe technology in China signals that strategic competitors are not just researching the technology but are actively fielding it. This increases the urgency for Western Governments and businesses to secure their own communications.

305. The Czech Government Has Publicly Attributed Cyberattacks to China

https://www.nukib.cz/en/about-us/news/the-czech-government-has-publicly-attributed-cyberattacks-to-china/

This official Government announcement attributes a cyberattack to a nation state actor known for "harvest now, decrypt later" tactics. This provides concrete, real world evidence of the primary threat scenario that PQC is designed to mitigate.

306. DARPA taps Microsoft, PsiQuantum for scalable quantum computer research

https://fcw.com/defense/2025/02/darpa-taps-microsoft-psiquantum-scalable-quantum-computer-research/394017/

This news article reports on DARPA's significant investment in building a large -scale quantum computer. This domestic R&D effort highlights the U.S. Government's dual interest in both creating quantum capabilities and defending against them with PQC.

307. The One Big Beautiful Bill Act: Comprehensive Holland & Knight Analysis

https://www.hklaw.com/-/media/files/insights/publications/2025/07/onebigbeautifulbillcomprehensiveanalysis.pdf

This legal analysis details the One Big Beautiful Bill Act, the landmark budget reconciliation package signed into law on July 4, 2025, which enacts sweeping policy and funding changes across defense, healthcare, tax, and energy. The document serves as a guide for organizations to navigate the bill's significant impacts, including major funding reallocations and the rescission of numerous clean energy initiatives from the Inflation Reduction Act.

308. H.R.1 - 119th Congress (2025-2026): The One Big Beautiful Bill Act

https://www.congress.gov/bill/119th-congress/house-bill/1/text/enr

This is the official Congress.gov page for the "One Big Beautiful Bill Act," the budget reconciliation package signed into law on July 4, 2025.

SECTION 18

The June 2026 Federal Mandate: Executive Orders, OMB M-26-15, and the DoW Strategy

309. Executive Order 14306: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 - GovInfo

https://www.govinfo.gov/app/details/DCPD-202500669

Issued June 6, 2025, this order amended Executive Order 14144 line by line while keeping its PQC provisions intact. It directed CISA and the National Security Agency to publish a list of PQC capable product categories by December 1, 2025 and required agencies to support Transport Layer Security 1.3 no later than January 2, 2030. The order reaffirmed the cryptanalytically relevant quantum computer threat framing of NSM-10, keeping quantum readiness a live procurement issue through the change in administration.

310. Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks - The White House

https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

Signed June 22, 2026, this is the centerpiece Federal PQC mandate. It sets December 31, 2030 for PQC key establishment on high value assets and high impact systems, December 31, 2031 for PQC digital signatures, and directs Federal Acquisition Regulation changes requiring Federal contractors to comply with PQC FIPS by the end of 2030. The order names harvest now, decrypt later collection as an active adversary practice, which makes it the anchor citation for every Federal PQC pursuit.

311. Executive Order 14412, Federal Register Publication (91 FR 38483) - Federal Register

https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks

The text of record, published June 25, 2026. Legal and compliance teams should work from the Federal Register version when determining precise requirements, definitions, and deadlines, since publication here gives the order the force of law.

312. Preparing for Q-Day: New Executive Orders Address Quantum Innovation and Post-Quantum Cryptography - K&L Gates

https://www.klgates.com/Preparing-for-Q-Day-New-Executive-Orders-Address-Quantum-Innovation-and-Post-Quantum-Cryptography-6-26-2026

Law firm analysis of both June 22, 2026 orders, including Executive Order 14413, Ushering in the Next Frontier of Quantum Innovation, which establishes the QC-ADDS effort to build a scientifically useful quantum computer. The analysis frames the pair as an update to the National Quantum Strategy, with offense and defense signed the same day, and helps executives understand how innovation funding and migration mandates interact.

313. Trump Administration Releases Two Executive Orders on Quantum - Covington, Inside Privacy

https://www.insideprivacy.com/cybersecurity-2/trump-administration-releases-two-executive-orders-on-quantum/

A second major law firm read on the June 2026 orders, continuing this index's pattern of pairing primary sources with expert legal interpretation. Covington grounds its analysis in the harvest now, decrypt later premise: information stolen today gets decrypted once the hardware arrives, so the confidentiality clock on long lived data started before Q-Day.

314. Securing the Nation Against Advanced Cryptographic Attacks, EO One Pager - House Republican Policy Committee

https://republicanpolicy.house.gov/sites/evo-subsites/republicanpolicy-evo.house.gov/files/evo-media-document/26-06-23-securing-the-nation-against-advanced-cryptographic-attacks-eo-one-pager-jo-approved.pdf

A congressional one pager summarizing Executive Order 14412: the threat, the OMB and National Cyber Director coordination roles, and the NIST, NSA, and CISA taskings. Useful as a briefing artifact for stakeholders who will not read the full order, and evidence that PQC now has visibility inside House policy machinery.

315. H.R. 9516, To Codify Executive Order 14412 (119th Congress) - Congress.gov

https://www.congress.gov/bill/119th-congress/house-bill/9516

Legislation to give Executive Order 14412 the force of law. Whatever its fate, the bill signals congressional intent to lock the 2030 and 2031 deadlines in place beyond any single administration, the same durability the Quantum Computing Cybersecurity Preparedness Act gave the inventory mandate.

316. OMB Memorandum M-26-15: Execution of the Migration to Post-Quantum Cryptography - The White House

https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

Issued June 24, 2026, this is the operational playbook implementing Executive Order 14412 for civilian agencies and the successor to M-23-02. It establishes a five phase schedule from 2026 through 2035, requires agencies to name PQC migration leads within 30 days and submit comprehensive migration plans within 120 days, mandates automated cryptographic inventory feeding a cryptographic bill of materials, makes crypto agility an architectural objective, and sets the goal of mitigating as much quantum risk as feasible by December 31, 2030. Contractors should map every offering to the phase their agency customer occupies.

317. OMB Issues Federal Roadmap for Post-Quantum Cryptography Migration - HSToday

https://www.hstoday.us/subject-matter-areas/cybersecurity/omb-issues-federal-roadmap-for-post-quantum-cryptography-migration/

Trade press summary of M-26-15 for readers who need the phased 2026 through 2035 schedule without the memo's technical appendices. It notes that OMB published the memorandum two days after the executive order signed, evidence that planning preceded the signature.

318. Department of War Post Quantum Cryptography Strategy - DoW Chief Information Officer

https://dodcio.defense.gov/Portals/0/Documents/Library/DoW-PQC-Strategy.pdf

The defense side companion to Executive Order 14412 and the first department wide PQC plan. All DoW systems must support PQC or be phased out by December 31, 2030 and must use PQC by December 31, 2031, with CNSA 2.0 as the baseline for National Security Systems. The strategy organizes work into five lines of effort and two acquisition tracks and explicitly rejects quantum key distribution, quantum networking, and preshared key overlays as substitutes for native asymmetric PQC. Defense contractors should treat those exclusions as a filter on solution architectures.

319. Securing Global Dominance: DoW Unleashes Quantum Defense Strategy - Department of War

https://www.war.gov/News/Releases/Release/Article/4524599/securing-global-dominance-dow-unleashes-quantum-defense-strategy-to-harden-netw/

The official release from DoW Chief Information Officer Kirsten Davies announcing the strategy, tied directly to the previous day's executive orders. Quote material for proposals and thought leadership on securing the tactical edge, satellite communications, and command and control.

320. War Department Details Post-Quantum Cryptography Roadmap - GovCIO Media & Research

https://govciomedia.com/war-department-details-post-quantum-cryptography-roadmap/

Reporting from TechNet Cyber 2026 with DISA engineers on execution. DISA identifies public key infrastructure modernization as step one and expects prototyping to change requirements as migration proceeds. For capture teams, this is the clearest public signal of where early defense PQC dollars land.

321. Uncertain Quantum Future Presents 'Existential Threat' to US Military Missions - DefenseScoop

https://defensescoop.com/2026/06/25/pentagon-pqc-strategy-post-quantum-cryptography/

Coverage of the strategy's threat framing: the Pentagon now describes fully realized quantum computing in adversary hands as an existential threat to US missions. That language, in an official strategy, gives proposal writers a citable severity anchor no vendor white paper can match.

SECTION 19

Congressional Action and Pending Legislation

322. S.3597, National Quantum Initiative Reauthorization Act of 2026 (119th Congress) - Congress.gov

https://www.congress.gov/bill/119th-congress/senate-bill/3597

The Senate vehicle for reauthorizing the National Quantum Initiative, introduced in January 2026 by Senators Cantwell and Young with bipartisan cosponsors and passed unanimously by the Senate Commerce Committee in April 2026. It extends the initiative through December 2034, adds quantum supply chain resilience mandates, creates new NIST quantum centers and NSF multidisciplinary research centers, and directs an international cooperation strategy with allies. The original authorization lapsed in 2023, so restoring the framework is a live congressional priority.

323. H.R. 8462, National Quantum Initiative Reauthorization Act (119th Congress) - Congress.gov

https://www.congress.gov/bill/119th-congress/house-bill/8462

The House companion, advanced by the Science, Space, and Technology Committee on April 29, 2026 by voice vote after adopting 12 amendments. One adopted amendment directs Federal agencies to assist state and local Governments with PQC migration planning and implementation, and the bill adds an NSF cryptography research section that names post quantum cryptography explicitly. Differences with the Senate bill must be reconciled before enactment, and sponsors have floated attaching reauthorization to the FY27 NDAA as a fallback path.

324. Cantwell, Young, Colleagues Introduce Bipartisan National Quantum Initiative Reauthorization Act - Senate Commerce Committee

https://www.commerce.senate.gov/2026/1/cantwell-young-colleagues-introduce-bipartisan-national-quantum-initiative-reauthorization-act

The introduction announcement from the Senate Commerce Committee, useful for the bill's framing and its sponsor list spanning both parties, including the Senate Majority Leader. Endorsements from IBM, Google Quantum AI, Microsoft, IonQ, PsiQuantum, and the Quantum Economic Development Consortium signal the breadth of the commercial coalition behind reauthorization.

325. S.2558, The National Quantum Cybersecurity Migration Strategy Act of 2025 (119th Congress) - Congress.gov

https://www.congress.gov/bill/119th-congress/senate-bill/2558

Introduced July 30, 2025 by Senators Peters and Blackburn, this bill would direct development of a National Quantum Cybersecurity Migration Strategy within 180 days through the ESIX subcommittee, stand up a post quantum pilot program with systems upgraded by January 1, 2027, survey agency migration costs, and require annual Comptroller General progress assessments. Its cost survey and pilot provisions would generate exactly the demand signals PQC service providers should track.

326. S.1346, Defense Quantum Acceleration Act of 2025 (119th Congress) - Congress.gov

https://www.congress.gov/bill/119th-congress/senate-bill/1346

Introduced by Senators Blackburn and Hassan, this bill would codify joint quantum information science transition activities and a Principal Quantum Advisor to move quantum technologies from research into operational use across the Department. An earlier version was dropped from the FY25 NDAA in conference, and the bill returned as a filed FY26 NDAA amendment, making it a persistent legislative vehicle worth tracking.

327. Lawmakers Have Filed Nearly a Dozen Quantum Amendments to FY26 NDAA - Nextgov/FCW

https://www.nextgov.com/emerging-tech/2025/09/lawmakers-have-filed-nearly-dozen-quantum-amendments-fy26-ndaa/408379/

Reporting on the quantum amendments filed to the FY26 NDAA, including a Strategy for Quantum Readiness for defense, an assessment of quantum resilient network migration, and inclusion of the National Quantum Cybersecurity Migration Strategy Act. The NDAA remains the most reliable annual vehicle for quantum and PQC policy, so amendment activity previews the mandates that arrive in final bill text.

328. US Quantum Policy: NQI Reauthorization and PQC Bills - Marin Ivezic, PostQuantum.com

https://postquantum.com/quantum-policy/us-quantum-legislation-dod-pqc-2026/

A running analysis of US quantum legislation as of spring 2026, covering the reauthorization markups, the adopted PQC amendments including state and local migration assistance, and quantum supply chain provisions such as helium 3 access. Useful for readers who need the legislative landscape assembled in one place between official bill texts.

SECTION 20

NIST Standards and Guidance Updates

329. PQC Standardization Process: Current Status - NIST Computer Security Resource Center

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

The authoritative status page for the standards themselves. FIPS 203, 204, and 205 published August 13, 2024. FN-DSA, derived from FALCON, will publish as FIPS 206 and remains in development, with finalization expected around late 2026 or 2027. HQC was selected March 11, 2025, with NIST IR 8545 documenting the fourth round evaluation, and a draft HQC standard is expected in 2026. The practical guidance is unchanged: deploy ML-KEM, ML-DSA, and SLH-DSA now and design for the algorithms still in the pipeline.

330. NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards - NIST

https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

The deprecation timeline itself. Quantum vulnerable public key algorithms at the 112 bit security level, including RSA-2048 and ECDSA P-256, are deprecated after 2030 and disallowed after 2035. Executive Order 14412 and M-26-15 now hang enforcement dates on the same posts, which makes this report the technical foundation of the Federal deadlines.

331. NIST SP 800-227 (Draft): Recommendations for Key-Encapsulation Mechanisms - NIST

https://csrc.nist.gov/pubs/sp/800/227/ipd

The first NIST recommendation dedicated to key encapsulation mechanisms, released for comment in January 2025. It pairs with FIPS 203 to tell implementers how to use ML-KEM correctly, covering key establishment patterns the FIPS itself leaves open. Engineering teams building to M-26-15 requirements will work from this document.

332. Migration to Post-Quantum Cryptography (NIST SP 1800-38) - NIST National Cybersecurity Center of Excellence

https://www.nccoe.nist.gov/projects/migration-post-quantum-cryptography

The NCCoE practice guide project, built with dozens of industry collaborators, covering cryptographic discovery tooling, interoperability, and performance testing of the finalized algorithms. The closest thing to a Federal reference implementation library, and the natural companion to the automated inventory requirement in M-26-15.

333. NIST IR 8545: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process - NIST

https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf

The formal record of the fourth round: why NIST selected the code based HQC over BIKE as the second key encapsulation mechanism and why Classic McEliece was not chosen. HQC deliberately rests on a different mathematical problem than ML-KEM, diversifying the portfolio against a future breakthrough in lattice cryptanalysis, with a draft standard expected around 2026 and finalization targeted for 2027. Architects should factor the two algorithm strategy into crypto agility designs.

SECTION 21

CISA and NSA Procurement Guidance

334. Product Categories for Technologies That Use Post-Quantum Cryptography Standards - CISA

https://www.cisa.gov/resources-tools/resources/product-categories-technologies-use-post-quantum-cryptography-standards

Released January 2026 in response to Executive Order 14306, compiled with NSA, and updated on a rolling basis. It identifies product categories where PQC capable products are widely available today, including cloud platform and infrastructure services, web browsers, messaging software, and full disk encryption, and instructs organizations to acquire only PQC capable products in those categories. The list now shapes Federal acquisition directly, and M-26-15 points agencies to this exact resource.

335. CISA Releases Product Categories List to Propel Post-Quantum Cryptography Adoption - CISA

https://www.cisa.gov/news-events/news/cisa-releases-product-categories-list-propel-post-quantum-cryptography-adoption-pursuant-president

The official announcement, with the acting CISA Director calling quantum computing a real and urgent threat to systems that rely on public key cryptography and urging organizations to prioritize PQC capable procurement. Quote material for executive briefings and proposal threat sections.

336. CNSA 2.0 Explained: PQC Requirements, Timelines, and Federal Impact - QuSecure

https://www.qusecure.com/cnsa-2-0-pqc-requirements-timelines-federal-impact/

Explains the December 2024 revision of CNSA 2.0, version 2.1, which updates the original 2022 NSA announcement cited earlier in this index. The DoW strategy names CNSA 2.0 as the required baseline for National Security Systems, so vendors serving the defense and intelligence sectors should track the revision cycle and the rejection of quantum key distribution as a compliance path.

SECTION 22

Protocol Standards and Internet Integration

337. Post-Quantum Hybrid ECDHE-MLKEM Key Agreement for TLS 1.3 (draft-ietf-tls-ecdhe-mlkem) - IETF TLS Working Group

https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/

The IETF standards track specification defining the hybrid key agreements X25519MLKEM768, SecP256r1MLKEM768, and SecP384r1MLKEM1024 for TLS 1.3. X25519MLKEM768 is the mechanism major browsers and content networks already deploy, so this document describes how a large share of the PQC protected traffic on today's internet actually works. Its authors span PQShield, AWS, Cloudflare, and the University of Waterloo, a snapshot of the industry coalition doing the engineering.

338. Hybrid Key Exchange in TLS 1.3 (draft-ietf-tls-hybrid-design) - IETF TLS Working Group

https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/

The companion framework document defining how classical and post quantum key exchanges combine in TLS 1.3 so a session remains secure as long as either component holds. Hybrid deployment is the consensus bridge strategy during migration, hedging against undiscovered weaknesses in the new algorithms while closing the harvest now, decrypt later window immediately.

SECTION 23

Quantum Algorithms and Cryptanalysis Research

339. An Efficient Quantum Factoring Algorithm - Oded Regev, arXiv

https://arxiv.org/abs/2308.06572

Regev's 2023 paper delivered the first substantial asymptotic improvement on Shor's algorithm in three decades, factoring an n bit integer with markedly smaller quantum circuits run multiple times and combined through classical post processing. Later work has proven the underlying number theory unconditionally and begun reducing the algorithm's memory overhead. Algorithmic progress compounds with hardware progress, which is one reason CRQC timeline estimates keep moving earlier rather than later.

340. Extending Regev's Factoring Algorithm to Compute Discrete Logarithms - Ekerå and Gärtner, arXiv

https://arxiv.org/abs/2311.05545

Extends Regev's multidimensional approach from factoring to the discrete logarithm problem, the mathematics underpinning Diffie Hellman and elliptic curve cryptography. The extension matters because elliptic curves, not RSA, protect most modern internet traffic, and NIST IR 8547 deprecates both families on the same 2030 and 2035 schedule.

341. KyberSlash: Exploiting Secret-Dependent Division Timings in Kyber Implementations - Bernstein et al., IACR Cryptology ePrint Archive

https://eprint.iacr.org/2024/1049

Bernstein and coauthors disclosed two timing vulnerabilities, present even in the official reference code of Kyber, the algorithm standardized as ML-KEM, allowing secret key recovery within minutes to hours on affected platforms. The flaws were responsibly disclosed and quickly patched across libraries. The lesson for implementers is that standardized algorithms are only as strong as their implementations, which is why validated cryptographic modules and side channel testing belong in every migration plan.

SECTION 24

Quantum Threat Research and Hardware Milestones

342. IBM Lays Out Clear Path to Fault-Tolerant Quantum Computing - IBM Quantum

https://www.ibm.com/quantum/blog/large-scale-ftqc

IBM's engineering roadmap to Starling, a large scale fault tolerant system targeted for 2029, with quantum advantage claimed for 2026. The 2025 Loon chip validates the quantum low density parity check architecture the plan depends on, and the 120 qubit Nighthawk processor shipped to users in late 2025. Hardware roadmaps now carry dates inside the Federal migration window, which retires the argument that agencies have time to wait.

343. Quantinuum Unveils Accelerated Roadmap to Universal, Fully Fault-Tolerant Quantum Computing by 2030 - Quantinuum

https://www.quantinuum.com/press-releases/quantinuum-unveils-accelerated-roadmap-to-achieve-universal-fault-tolerant-quantum-computing-by-2030

The trapped ion route to fault tolerance by 2030 through the Apollo system. Quantinuum's Helios machine demonstrated 48 logical qubits from 98 physical qubits in November 2025, a 2 to 1 ratio against the hundreds to one overhead long assumed for surface codes. Error correction efficiency, not raw qubit counts, is now the number for risk officers to watch.

344. Quantum Error Correction Below the Surface Code Threshold - Google Quantum AI, Nature

https://www.nature.com/articles/s41586-024-08449-y

The December 2024 Nature paper in which Google demonstrated quantum error correction below the surface code threshold on the 105 qubit Willow processor, with logical error rates halving at each increase in code distance and real time decoding. Below threshold operation had been the field's defining goal since the 1990s; crossing it converted fault tolerant quantum computing from an open scientific question into an engineering program.

345. Meet Willow, Our State-of-the-Art Quantum Chip - Google

https://blog.google/innovation-and-ai/technology/research/google-willow-quantum-chip/

The accessible companion announcement for Willow, including the benchmark in which the chip completed in under five minutes a sampling task estimated to take today's fastest supercomputer ten septillion years. Useful for executive audiences who need the significance of below threshold error correction without the physics.

346. Caltech Team Sets Record with 6100-Qubit Array - Caltech

https://www.caltech.edu/about/news/caltech-team-sets-record-with-6100-qubit-array

Caltech physicists assembled 6,100 neutral atom qubits in an optical tweezer array, published in Nature in September 2025, with roughly 13 second coherence times and 99.98 percent control fidelity, about ten times larger than previous arrays of the kind. Scale and quality advancing together across superconducting, trapped ion, and neutral atom platforms is the pattern risk officers should read as schedule pressure on the cryptographic transition.

347. Microsoft Unveils Majorana 1, the World's First Quantum Processor Powered by Topological Qubits - Microsoft Azure Quantum

https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

Microsoft's February 2025 announcement of Majorana 1, a processor built on claimed topological qubits and a materials stack designed to scale toward a million qubits on a single chip, published alongside a Nature paper. Independent physicists continue to dispute whether the results demonstrate the Majorana zero modes the approach requires, and Nature's own review file stopped short of endorsing that claim. The entry is included both for the engineering ambition and as a reminder that extraordinary quantum claims deserve scrutiny of the underlying evidence.

SECTION 25

Industry Deployment and Market Acceleration

348. Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms - Microsoft Security

https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-apis-now-generally-available-on-microsoft-platforms/4469093

As of November 2025, ML-KEM and ML-DSA are generally available in Windows 11, Windows Server 2025, and .NET 10, delivered through the Cryptography API: Next Generation layer with support for hybrid and composite certificates. PQC now ships in the default enterprise stack rather than in specialist toolkits, which removes the largest practical objection to starting migration.

349. New Windows Features to Secure Today's Data in a Post-Quantum World - Microsoft Security

https://techcommunity.microsoft.com/blog/microsoft-security-blog/new-windows-features-to-secure-today%E2%80%99s-data-in-a-post-quantum-world/4523370

The July 2026 follow up: Active Directory Certificate Services issues ML-DSA certificates as of May 2026, extending PQC into enterprise public key infrastructure, certification authorities, and Online Certificate Status Protocol responders. The commercial tooling for the PKI first migration step now exists off the shelf.

350. Microsoft Moves Up Quantum-Safe Security Deadline to 2029 - The Quantum Insider

https://thequantuminsider.com/2026/07/01/microsoft-moves-up-quantum-safe-security-deadline-to-2029/

In July 2026 Microsoft accelerated its Quantum Safe Program completion date from 2033 to 2029, citing Executive Order 14412 and France's decision that its national cybersecurity agency will stop certifying security products lacking quantum resistant encryption from 2027. Google and Cloudflare hold matching 2029 targets. When the largest platform vendors converge on dates ahead of Government deadlines, laggards inherit compatibility risk as well as security risk.

351. The White House's Post-Quantum Executive Order Is an Important Milestone. It's Time to Get to Work - Cloudflare

https://blog.cloudflare.com/post-quantum-eo-2026/

The internet infrastructure operator's analysis of Executive Order 14412, including the contractor FIPS requirement and the 2030 and 2031 deadlines. Cloudflare frames Federal procurement as the historical lever that drives industry wide technology adoption, the same argument that applies to commercial clients watching the Federal market.

352. The Complete US Post-Quantum Cryptography (PQC) Regulatory Framework in 2026 - Marin Ivezic, PostQuantum.com

https://postquantum.com/security-pqc/us-pqc-regulatory-framework-2026/

Maps the full regulatory stack, including sector activity beyond the executive branch: the G7 Cyber Expert Group financial sector PQC roadmap of January 13, 2026, co chaired by the US Treasury and the Bank of England; Securities and Exchange Commission references to NIST algorithms in digital asset custody proposals; and PQC disclosures appearing in S-1 registration statements. Quantum readiness is turning into a material disclosure issue, which puts boards on the hook alongside chief information security officers.

353. US Federal PQC Mandate After June 2026: Complete Guide - Marin Ivezic, PostQuantum.com

https://postquantum.com/post-quantum/us-federal-pqc-mandate-2026/

A single synthesis of how Executive Order 14412, Executive Order 14413, M-26-15, and the DoW strategy interlock: governance, mandate, implementation guidance, and offense investment as dependent layers. The right orientation read before the primary sources in this index.

SECTION 26

International and Financial Sector Coordination

354. G7 Cyber Expert Group Releases Roadmap for Coordinating the Transition to Post-Quantum Cryptography in the Financial Sector - US Department of the Treasury

https://home.treasury.gov/news/press-releases/sb0355

The official announcement of the G7 Cyber Expert Group roadmap, released January 12, 2026 under co chairs the US Department of the Treasury and the Bank of England. The co chairs warn that quantum capable decryption presents a significant risk to the safety and soundness of the financial ecosystem, language that moves quantum readiness into prudential regulator territory and onto bank board agendas.

355. G7 Cyber Expert Group Statement: Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector - US Department of the Treasury

https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

The roadmap itself: a phased, risk based migration framework for financial institutions, authorities, and their technology vendors covering awareness, discovery and inventory, risk assessment and planning, migration execution, and ongoing validation. It cites 2035 as the emerging international target for full migration, with the most critical systems upgraded around 2030 to 2032, aligning the global financial sector with the US Federal timeline.

About Tanaq Integrated Technologies

Preparing for the quantum transition

Tanaq Integrated Technologies is the technology division of St. George Tanaq Corporation, an Alaska Native Corporation. Federal work is delivered through Tanaq Technical Services, LLC,

a certified Alaska Native 8(a) small business with a contract security program and ISO 9001:2015 certification.

Our post quantum practice covers cryptographic discovery and inventory, quantum risk prioritization, harvest now decrypt later protection, crypto agile architecture, hybrid cryptographic migration, network and gateway protection, identity and certificate integration, legacy and operational technology isolation, and compliance, training, and sustainment.

CONTACT

Ammanda Paige, Senior Executive Director and General Manager
apaige@tanaq.com | (301) 433-3343
3201 C Street, Suite 602, Anchorage, AK 99503
tanaq.com/tanaq-integrated-technology

Tanaq
INTEGRATED TECHNOLOGIES DIVISION

Roger Payne is President of Tanaq Integrated Technologies.

Copyright © 2025-2026 Tanaq Technical Services. All rights reserved.