ZRA

zeichner risk analytics

# Future of Cybersecurity

## Leadership Needed to Fully Define Quantum Threat Computing Strategy

This white paper is for informational purposes only and is not intended to provide legal, financial, business, or professional advice. Zeichner Risk Analytics, LLC (ZRA) makes no representations or warranties, express or implied, regarding the accuracy, completeness, or reliability of the information contained herein. Readers should consult with appropriate professionals before making any decisions or taking any actions based on this publication.

ZRA shall not be held liable for any direct, indirect, incidental, or consequential damages arising from the use of or reliance on the information in this white paper.

As used in this document, “ZRA” refers to Zeichner Risk Analytics, LLC. Please visit www.zra.com for more information about our company and services.

# Table of Contents

# Introduction

For the future of cybersecurity, the U.S. Government Accountability Office (GAO), in a report written on November 21, 2024, determined that leadership is needed to fully develop a strategy for threat mitigation. In this study, the GAO was asked to examine the federal government's strategy for addressing the threat quantum computers pose to cryptography in unclassified systems.

Cryptography is the practice of securing information by transforming it using mathematical functions. These functions generate a series of letters and numbers known as keys. Public key cryptography is a widely used method of protecting information with two different keys: a public key and a private key. Federal agencies and critical infrastructure owners rely on public key cryptography to secure sensitive data and personally identifiable information within their technology systems.

# Quantum Computer Capabilities

Quantum computers leverage the properties of qubits, the quantum equivalent of classical computing bits, to solve certain problems significantly faster than traditional computers. However, some experts predict that a cryptographically relevant quantum computer (CRQC), capable of breaking public key cryptography, will take 10 to 20 years to develop. Therefore, agencies and critical infrastructure face an increased security risk if they rely solely on cryptography and fail to start preparing now.

The capabilities of quantum computers threaten the nation's cryptography by compromising the confidentiality, integrity, and availability of systems that rely on cryptographic protection. In response, several strategies have been proposed to mitigate these risks. International organizations promote the adoption of post-quantum cryptography (PQC), which is designed to withstand quantum computing threats. For example, the Group of Seven (G7) and the North Atlantic Treaty Organization (NATO) advocate for the adoption of PQC. However, other organizations, such as the Internet Engineering Task Force (IETF) and the European Union, suggest a hybrid approach that combines PQC with classical cryptographic methods.

# Defense National Strategies

The U.S. strategy documents partially address the key characteristics of an effective national strategy, as identified in previous GAO research. Based on an analysis of these documents, the GAO identified three central goals:

1. Standardize post-quantum cryptography.
2. Transition federal systems to post-quantum cryptography.
3. Encourage all sectors of the economy to prepare for the quantum threat.

A national defense strategy should include six essential characteristics:

1. Purpose, scope, and methodology: Explains why the strategy was created, its scope, and the development process.
2. Problem definition and risk assessment: Identifies national security concerns, analyzes threats and vulnerabilities, and assesses risks to critical infrastructure.
3. Objectives, activities, milestones, and performance measures: Defines objectives, outlines key activities, sets priorities, and establishes performance benchmarks.
4. Resources, investments, and risk management: Summarizes costs, identifies funding sources, and balances risk reduction with financial considerations.
5. Operational roles, responsibilities, and coordination: Specifies who is responsible for implementation, outlines their roles, and details coordination mechanisms.
6. Implementation and integration: Describes how the strategy will be executed and how it aligns with other national and international cybersecurity initiatives.

The U.S. government's quantum computing cybersecurity strategy only partially addresses these six characteristics. Each element of the strategy has unique strengths and weaknesses:

- Purpose, scope, and methodology: While some PQC standard documents describe their development process, others lack clear methodology or processes.

- Problem definition and risk assessment: Many documents do not fully define CRQC or predict when it will become relevant. One document does assess the risk of CRQC across all 55 national critical functions tied to critical infrastructure.

- Objectives, activities, milestones, and performance measures: The strategy outlines objectives and activities for standardizing PQC and transitioning federal agencies but does not fully address the final goal of widespread adoption. Performance measures are not clearly defined.

- Resources, investments, and risk management: The strategy identifies costs related to transitioning federal agencies to PQC but does not specify funding sources for other objectives. Risk management is partially addressed, focusing on prioritizing system transitions to minimize exposure.

- Operational roles, responsibilities, and coordination: The documents outline strategies for implementing the first two goals but do not clarify responsibilities for achieving the third goal. However, coordination mechanisms are provided for all three goals.

- Implementation and integration: The strategy documents reference other related documents, showing integration, but they provide implementation plans only for the first two goals.

# Recommendations for ONCD

No single federal agency is responsible for coordinating the U.S. national quantum computing cybersecurity strategy. In January 2021, Congress established the Office of the National Cyber Director (ONCD), which has the authority to take on this role. The GAO recommends that the National Cyber Director:

1. Lead the coordination of the U.S. national quantum computing cybersecurity strategy.

2. Ensure that the strategy's various documents address all the essential characteristics of an effective national strategy.

Additionally, the Director must regularly report cybersecurity threats to Congress, as required by federal law.

In December 2024, three researchers from the Center for Cybersecurity Policy and Law (CCPL) published an updated vision for the ONCD. In July 2024, the Senate introduced bipartisan legislation to establish a unified framework for streamlining cybersecurity regulations across the federal government. This proposed bill aims to address challenges arising from overlapping cybersecurity regulations by creating an interagency harmonization committee, chaired by the ONCD.

A month before the second Trump administration took office, the CCPL recommended that the newly nominated National Cyber Director—revealed in February 2025 as Sean Cairncross—address some of these challenges. The nominee is also expected to define the structure of the ONCD. Additionally, Congress will need to collaborate with the administration to clearly outline the ONCD's roles and authorities moving forward. The CCPL provided five key recommendations for the new NCD nominee, Sean Cairncross:

1. The White House should update and clarify the ONCD mission statement, clearly defining the policymaking responsibilities of the NCD in relation to other senior cyber leadership.

2. Congress should codify the NCD's role as the U.S. government's lead external-facing cyber official.

3. The White House should improve collaboration between the ONCD and the National Security Council (NSC) by appointing a dual-hatted senior director. The NSC/Cyber team should function similarly to NSC/Intecon to enhance coordination.

4. The NCD should staff the ONCD with more agency detailers and subject matter experts from both the government and the private sector.

5. Congress should codify the position of the Federal Chief Information Security Officer (CISO) within the Office of Management and Budget (OMB) and designate the Federal CISO as a direct report to the NCD.

# Conclusion

The future of cybersecurity, particularly in the face of emerging quantum computing threats, demands decisive leadership and a well-defined national strategy. While progress has been made in standardizing post-quantum cryptography and transitioning federal systems, significant gaps remain in risk assessment, resource allocation, and performance measurement. Without a unified federal effort, the nation's critical infrastructure remains vulnerable to future cryptographic threats.

The Office of the National Cyber Director must take the lead in coordinating a comprehensive strategy that fully addresses all six essential characteristics of an effective national cybersecurity plan. By ensuring a proactive approach, the U.S. can mitigate the risks posed by cryptographically relevant quantum computers and safeguard its digital infrastructure for years to come.

# Endnotes

**Government Report:**

U.S. Gov't Accountability Off., Cybersecurity: *Federal Agencies Need to Strengthen Their Incident Response Capabilities*, GAO-25-107703 (2025), https://www.gao.gov/assets/gao-25-107703.pdf.

**Policy Report:**

Ari Schwartz, Ines Jordan-Zoob & Samara Friedman, *Through the Looking Glass: An Updated Vision for the Office of the National Cyber Director*, Ctr. for Cybersecurity Pol'y & L. (Dec. 11, 2024), https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/67589ea3f1a160cf31996f8c_CCPL%20-%20ONCD_Final.pdf, https://www.centerforcybersecuritypolicy.org/insights-and-research/through-the-looking-glass-an-updated-vision-for-the-office-of-the-national-cyber-director.

**News Article:**

Weslan Hansen, *Trump Nominates Sean Cairncross as National Cyber Director, MeriTalk* (Feb. 13, 2025), https://www.meritalk.com/articles/trump-nominates-sean-cairncross-as-national-cyber-director/.

# For more information, contact:

## Authors

Lee Zeichner
CEO
lee@zra.com
(703) 868-8769

Zeichner Risk Analytics

4601 Fairfax Dr #1130, Arlington, VA 22203
(703) 351-1101

5661 Beaumont Avenue, San Diego, CA 92037
(703) 868-8769