BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

MEMORANDUM FOR THE VICE PRESIDENT

THE SECRETARY OF STATE

THE SECRETARY OF THE TREASURY

THE SECRETARY OF DEFENSE

THE ATTORNEY GENERAL

THE SECRETARY OF COMMERCE

THE SECRETARY OF ENERGY

THE SECRETARY OF HOMELAND SECURITY

THE ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF

THE DIRECTOR OF THE OFFICE OF MANAGEMENT BUDGET

THE DIRECTOR OF NATIONAL INTELLIGENCE

THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY

THE ASSISTANT TO THE PRESIDENT FOR NATIONAL

SECURITY AFFAIRS

THE COUNSEL TO THE PRESIDENT

THE ASSISTANT TO THE PRESIDENT FOR ECONOMIC POLICY AND DIRECTOR OF THE NATIONAL ECONOMIC COUNCIL

THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

THE NATIONAL CYBER DIRECTOR

THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF

THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION

THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SUBJECT: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

This memorandum outlines my Administration's policies and initiatives related to quantum computing. It identifies key steps needed to maintain the Nation's competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national security. It directs specific actions for agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to

quantum-resistant cryptography. A classified annex to this memorandum addresses sensitive national security issues.

Section 1. Policy. (a) Quantum computers hold the potential to drive innovations across the American economy, from fields as diverse as materials science and pharmaceuticals to finance and energy. While the full range of applications of quantum computers is still unknown, it is nevertheless clear that America's continued technological and scientific leadership will depend, at least in part, on the Nation's ability to maintain a competitive advantage in quantum computing and QIS.

(b) Yet alongside its potential benefits, quantum computing also poses significant risks to the economic and national security of the United States. Most notably, a quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions.

(c) In order to balance the competing opportunities and risks of quantum computers, it is the policy of my Administration: (1) to maintain United States leadership in QIS, through continued investment, partnerships, and a balanced approach to technology promotion and protection; and (2) to mitigate the threat of CRQCs through a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum resistant cryptography.

(d) Additional guidance and directives may be required in the future as quantum computing technologies and their associated risks mature.

Sec. 2. Promoting United States Leadership. (a) The United States must pursue a whole-of-government and whole of society strategy to harness the economic and scientific benefits of QIS, and the security enhancements provided by quantum-resistant cryptography. This strategy will require a coordinated, proactive approach to QIS research and development (R&D), an expansion of education and workforce programs, and a focus on developing and strengthening partnerships with industry, academic institutions, allies, and like-minded nations.

(b) The United States must seek to encourage transformative and fundamental scientific discoveries through investments in core QIS research programs. Investments should target the discovery of new quantum applications, new approaches to quantum-component

manufacturing, and advances in quantum enabling technologies, such as photonics, nanofabrication, and cryogenic and semiconductor systems.

(c) The United States must seek to foster the next generation of scientists and engineers with quantum-relevant skill sets, including those relevant to quantum-resistant cryptography. Education in QIS and related cybersecurity principles should be incorporated into academic curricula at all levels of schooling to support the growth of a diverse domestic workforce. Furthermore, it is vital that we attract and retain talent and encourage career opportunities that keep quantum experts employed domestically.

(d) To promote the development of quantum technology and the effective deployment of quantum-resistant cryptography, the United States must establish partnerships with industry; academia; and State, local, Tribal, and territorial (SLTT) governments. These partnerships should advance joint R&D initiatives and streamline mechanisms for technology transfer between industry and government.

(e) The United States must promote professional and academic collaborations with overseas allies and partners. This international engagement is essential for identifying and following global QIS trends and for harmonizing quantum security and protection programs.

(f) In support of these goals, within 90 days of the date of this memorandum, agencies that fund research in, develop, or acquire quantum computers shall coordinate with the Director of the Office of Science and Technology Policy to ensure a coherent national strategy for QIS promotion and technology protection, including for workforce issues. To facilitate this coordination, all such agencies shall identify a liaison to the National Quantum Coordination Office to share information and best practices, consistent with section 102(b)(3) of the National Quantum Initiative Act (Public Law 115-368) and section 6606 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81). All coordination efforts shall be undertaken with appropriate protections for sensitive and classified information and intelligence sources and methods.

Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035. Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for

quantum resistant cryptography for their respective jurisdictions. The first sets of these standards are expected to be released publicly by 2024.

(b) Central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards. This effort is an imperative across all sectors of the United States economy, from government to critical infrastructure, commercial services to cloud providers, and everywhere else that vulnerable public-key cryptography is used.

(c) Consistent with these goals:

(i) Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall initiate an open working group with industry, including critical infrastructure owners and operators, and other stakeholders, as determined by the Director of NIST, to further advance adoption of quantum-resistant cryptography. This working group shall identify needed tools and data sets, and other considerations to inform the development by NIST of guidance and best practices to assist with quantum resistant cryptography planning and prioritization. Findings of this working group shall be provided, on an ongoing basis, to the Director of the Office of Management and Budget (OMB), the Assistant to the President for National Security Affairs (APNSA), and the National Cyber Director to incorporate into planning efforts.

(ii) Within 90 days of the date of this memorandum, the Secretary of Commerce, through the Director of NIST, shall establish a "Migration to Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence to work with the private sector to address cybersecurity challenges posed by the transition to quantum-resistant cryptography. This project shall develop programs for discovery and remediation of any system that does not use quantum-resistant cryptography or that remains dependent on vulnerable systems.

(iii) Within 180 days of the date of this memorandum, and annually thereafter, the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), and in coordination with Sector Risk Management Agencies, shall engage with critical infrastructure and SLTT partners regarding the risks posed by quantum computers, and shall provide an annual report to the Director of OMB, the APNSA, and the National Cyber Director that includes recommendations for accelerating those entities' migration to quantum-resistant cryptography.

(iv) Within 180 days of the date of this memorandum, and on an ongoing basis, the Director of OMB, in consultation with the Director of CISA, the Director of NIST, the National Cyber

Director, and the Director of NSA, shall establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems (NSS). These requirements shall include a list of key information technology (IT) assets to prioritize, interim benchmarks, and a common (and preferably automated) assessment process for evaluating progress on quantum-resistant cryptographic migration in IT systems.

(v) Within 1 year of the date of this memorandum, and on an annual basis thereafter, the heads of all Federal Civilian Executive Branch (FCEB) Agencies shall deliver to the Director of CISA and the National Cyber Director an inventory of their IT systems that remain vulnerable to CRQCs, with a particular focus on High Value Assets and High Impact Systems. Inventories should include current cryptographic methods used on IT systems, including system administrator protocols, non-security software and firmware that require upgraded digital signatures, and information on other key assets.

(vi) By October 18, 2023, and on an annual basis thereafter, the National Cyber Director shall, based on the inventories described in subsection 3(c)(v) of this memorandum and in coordination with the Director of CISA and the Director of NIST, deliver a status report to the APNSA and the Director of OMB on progress made by FCEB Agencies on their migration of non-NSS IT systems to quantum-resistant cryptography. This status report shall include an assessment of the funding necessary to secure vulnerable IT systems from the threat posed by adversarial access to quantum computers, a description and analysis of ongoing coordination efforts, and a strategy and timeline for meeting proposed milestones.

(vii) Within 90 days of the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, and on an annual basis thereafter, as needed, the Secretary of Commerce, through the Director of NIST, shall release a proposed timeline for the deprecation of quantum-vulnerable cryptography in standards, with the goal of moving the maximum number of systems off quantum-vulnerable cryptography within a decade of the publication of the initial set of standards. The Director of NIST shall work with the appropriate technical standards bodies to encourage interoperability of commercial cryptographic approaches.

(viii) Within 1 year of the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, the Director of OMB, in coordination with the Director of CISA and the Director of NIST, shall issue a policy memorandum requiring FCEB Agencies to develop a plan to upgrade their non-NSS IT systems to quantum-resistant cryptography. These plans shall be expeditiously developed and be designed to address the most significant risks first. The Director of OMB shall work with the head of each FCEB Agency to estimate the costs to upgrade vulnerable systems beyond already

planned expenditures, ensure that each plan is coordinated and shared among relevant agencies to assess interoperability between solutions, and coordinate with the National Cyber Director to ensure plans are updated accordingly.

(ix) Until the release of the first set of NIST standards for quantum-resistant cryptography referenced in subsection 3(a) of this memorandum, the heads of FCEB Agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations. However, to assist with anticipating potential compatibility issues, the heads of such FCEB Agencies should conduct tests of commercial solutions that have implemented pre-standardized quantum-resistant cryptographic algorithms. These tests will help identify interoperability or performance issues that may occur in Federal environments at an early stage and will contribute to the mitigation of those issues. The heads of such FCEB Agencies should continue to implement and, where needed, upgrade existing cryptographic implementations, but should transition to quantum-resistant cryptography only once the first set of NIST standards for quantum-resistant cryptography is complete and implemented in commercial products. Conformance with international standards should be encouraged, and may be required for interoperability.

(x) Within 1 year of the date of this memorandum, and annually thereafter, the Director of NSA, serving in its capacity as the National Manager, in consultation with the Secretary of Defense and the Director of National Intelligence, shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS. This guidance shall be consistent with National Security Memorandum/NSM-8 (Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems). The National Manager shall share best practices and lessons learned with the Director of OMB and the National Cyber Director, as appropriate.

(xi) Within 1 year of the date of this memorandum, and on an ongoing basis, and consistent with section 1 of NSM-8, the heads of agencies operating NSS shall identify and document all instances where quantum-vulnerable cryptography is used by NSS and shall provide this information to the National Manager.

(xii) Within 180 days of issuance by the National Manager of its standards on quantum-resistant cryptography referenced in section 3(a) of this memorandum, and annually thereafter, the National Manager shall release an official timeline for the deprecation of vulnerable cryptography in NSS, until the migration to quantum-resistant cryptography is completed.

(xiii) Within 1 year of issuance by the National Manager of its standards on quantum-resistant cryptography for referenced in subsection 3(a) of this memorandum, and annually thereafter,

the heads of agencies operating or maintaining NSS shall submit to the National Manager, and, as appropriate, the Department of Defense Chief Information Officer or the Intelligence Community Chief Information Officer, depending on their respective jurisdictions, an initial plan to transition to quantum resistant cryptography in all NSS. These plans shall be updated annually and shall include relevant milestones, schedules, authorities, impediments, funding requirements, and exceptions authorized by the head of the agency in accordance with section 3 of NSM-8 and guidance from the National Manager.

(xiv) By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate and in consultation with the National Manager. Implementation should seek to avoid interference with interoperability or other cryptographic modernization efforts.

(xv) By December 31, 2023, the Secretary of Defense shall deliver to the APNSA and the Director of OMB an assessment of the risks of quantum computing to the defense industrial base and to defense supply chains, along with a plan to engage with key commercial entities to upgrade their IT systems to achieve quantum resistance.

Sec. 4. Protecting United States Technology. (a) In addition to promoting quantum leadership and mitigating the risks of CRQCs, the United States Government must work to safeguard relevant quantum R&D and intellectual property (IP) and to protect relevant enabling technologies and materials. Protection mechanisms will vary, but may include counterintelligence measures, well-targeted export controls, and campaigns to educate industry and academia on the threat of cybercrime and IP theft.

(b) All agencies responsible for either promoting or protecting QIS and related technologies should understand the security implications of adversarial use and consider those security implications when implementing new policies, programs, and projects.

(c) The United States should ensure the protection of U.S. developed quantum technologies from theft by our adversaries. This will require campaigns to educate industry, academia, and SLTT partners on the threat of IP theft and on the importance of strong compliance, insider threat detection, and cybersecurity programs for quantum technologies. As appropriate, Federal law enforcement agencies and other relevant agencies should investigate and prosecute actors who engage in the theft of quantum trade secrets or who violate United States export control laws. To support efforts to safeguard sensitive information, Federal law

enforcement agencies should exchange relevant threat information with agencies responsible for developing and promoting quantum technologies.

(d) Consistent with these goals, by December 31, 2022, the heads of agencies that fund research in, develop, or acquire quantum computers or related QIS technologies shall develop comprehensive technology protection plans to safeguard QIS R&D, acquisition, and user access. Plans shall be coordinated across agencies, including with Federal law enforcement, to safeguard quantum computing R&D and IP, acquisition, and user access. These plans shall be updated annually and provided to the APNSA, the Director of OMB, and the Co-Chairs of the National Science and Technology Council Subcommittee on Economic and Security Implications of Quantum Science.

Sec. 5. Definitions. For purposes of this memorandum:

(a) the term "agency" has the meaning ascribed to it under 44 U.S.C. 3502;

(b) the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on the Nation's security, economy, public health and safety, or any combination thereof;

(c) the term "cryptographic agility" means a design feature that enables future updates to cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure;

(d) the term "cryptanalytically relevant quantum computer" or "CRQC" means a quantum computer capable of undermining current public-key cryptographic algorithms;

(e) the term "Federal Civilian Executive Branch Agency" or "FCEB Agency" means any agency except the Department of Defense or agencies in the Intelligence Community;

(f) the term "high value asset" means information or an information system that is so critical to an organization that the loss or corruption of this information, or loss of access to the system, would have serious impacts on the organization's ability to perform its mission or conduct business;

(g) the term "high impact system" means an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards (FIPS) 199 potential impact value of "high";

(h) the term “information technology” or “IT” has the meaning ascribed to it under 44 U.S.C. 3502;

(i) the term “National Security Systems” or “NSS” has the meaning ascribed to it in 44 U.S.C 3552(b)(6) and shall also include other Department of Defense and Intelligence Community systems, as described in 44 U.S.C. 3553(e)(2) and 44 U.S.C. 3553(e)(3);

(j) the term “quantum computer” means a computer utilizing the collective properties of quantum states, such as superposition, interference and entanglement, to perform calculations. The foundations in quantum physics give a quantum computer the ability to solve a subset of hard mathematical problems at a much faster rate than a classical (i.e., non quantum) computer;

(k) the term “quantum information sciences” or “QIS” has the meaning ascribed to it under 15 U.S.C. 8801(6) and means the study and application of the laws of quantum physics for the storage, transmission, manipulation, computing, or measurement of information; and

(l) the term “quantum-resistant cryptography” means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a CRQC or classical computer. This is also referred to as post-quantum cryptography.

Sec. 6. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof, to include the protection of intelligence sources and methods; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum shall also be implemented without impeding the conduct or support of intelligence activities, and all implementation measures shall be designed to be consistent with appropriate protections for sensitive information and intelligence sources and methods.

(d) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.