EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

I. OVERVIEW

Federal agencies[2] ("agencies") are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)[3] and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).[4] This paradigm shift relies in part on the ubiquitous use of strong encryption throughout agencies.

As outlined in NSM-10, the threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC)[5] requires that agencies prepare now to implement post-quantum cryptography (PQC). Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems. Additionally, agencies must remain cognizant that encrypted data can be recorded now and later decrypted by operators of a future CRQC.

[1] Available at: https://www.whitehouse.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/
[2] The term "agency" has the meaning given in 44 U.S.C. § 3502.
[3] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[4] Available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[5] Defined as quantum computers that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a classical computer.

This memorandum describes preparatory steps for agencies to undertake as they begin their transition to PQC by conducting a prioritized inventory of cryptographic systems. Further, this memorandum provides transitional guidance to agencies in the period before PQC standards are finalized by the National Institute of Standards and Technology (NIST), after which OMB will issue further guidance.

II. PRIORITIZED INVENTORY OF CRYPTOGRAPHIC SYSTEMS

A. Requirements

As per NSM-10, "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."

To achieve this, OMB, in coordination with the Office of the National Cyber Director (ONCD), and as directed by NSM-10, is to "establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems." NSM-10 also directs OMB to instruct agencies on how to prioritize their inventories. Accordingly, this memorandum establishes requirements for agencies to inventory their active cryptographic systems, with a focus on High Value Assets (HVAs) and high impact systems.[6] As used in this memorandum, the term "cryptographic system" means an active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: (1) creation and exchange of encryption keys; (2) encrypted connections; or (3) creation and validation of digital signatures.

By May 4, 2023, and annually thereafter until 2035, or as directed by superseding guidance, agencies are directed to submit a prioritized inventory of information systems and assets, excluding national security systems,[7] that contain CRQC-vulnerable cryptographic systems to ONCD and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).[8]

The inventory must encompass each information system or asset that is **any** of the following, whether operated by the agency or on the agency's behalf:[9]

- A high impact information system;
- An agency HVA; or
- Any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks.[10] Agencies should include information systems or assets that:

[6] Defined by NSM-10 as "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.'"

[7] For the purposes of this memorandum, "national security system" refers both to any information system described in 44 U.S.C. § 3552(b)(6), as well as any system described in 44 U.S.C. § 3553(e)(2) or (e)(3).

[8] As outlined in Appendix B.

[9] This inventory should not include any national security systems.

[10] Agencies are encouraged to consult with CISA to help make these determinations.

- Contain data expected to remain mission-sensitive in 2035;[11] or
- Are logical access control systems based in asymmetric encryption (such as Public Key Infrastructure) that use any of the algorithms listed in Appendix B.

Initially, agencies should focus their inventory on their most sensitive systems. OMB expects to direct inventory by agencies of systems or assets not in the above scope through future guidance on Federal Information System Modernization Act of 2014[12] requirements. At this point in time, those systems need not be included in the inventory submitted to ONCD and CISA.

For each information system or asset included in the ONCD/CISA inventory, agencies must provide the following:

1. Federal Information Security Modernization Act (FISMA) system identifier.[13]
2. The Federal Information Processing Standard (FIPS) 199[14] system categorization (Low, Moderate, or High).
3. If an HVA, the HVA identifier.
4. Each CRQC-vulnerable cryptographic system actively used[15] by the information system or asset, including the:
   - Cryptographic algorithm used;[16]
   - Service provided by the cryptographic system; and
   - Length of associated cryptographic keys or modules.
5. If the cryptographic system(s) is/are part of a software package, indicate whether the software package is:
   - Commercial-Off-the-Shelf (COTS) and name of the vendor;
   - Government-Off-the-Shelf (GOTS) and name of the vendor; or
   - Other (e.g., custom software) and name of the vendor/developer.
6. Operating system(s), including major and minor version information, if applicable.
7. Whether the information system or hosting information system(s) is/are hosted by:
   - The agency (on premise);
   - A commercially operated cloud service provider, in which case the name of the commercial provider must be supplied;[17]

[11] This criterion refers to data that if recorded now, and later decrypted by a CRQC in 2035, would still be considered mission sensitive.
[12] 44 U.S.C. §§ 3551 et seq. See also § 3552(b)(3)
[13] Agencies shall only submit identifiers for systems and HVAs and shall not include names that identify the function or logical or physical location of the system or asset.
[14] Available at: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
[15] For the purposes of this memo, "actively used" means that it is possible for the cryptographic system to be employed during operation of the overall system, even if the cryptographic system is not employed during routine use (for example, if it is only employed to support legacy clients).
[16] For a list of CQRC-vulnerable algorithms, see Appendix B.
[17] For cloud products or services accredited by FedRAMP, agencies should work with the FedRAMP PMO to obtain a cryptographic implementation inventory.

    - A Government-operated cloud service provider, in which case the name of the agency provider must be supplied; or
    - A hybrid environment, in which case the name of the cloud service provider(s) must be supplied.
8. Lifecycle characteristics of the data contained in the system, including types of data (as described by national records management categories) and how long the data and associated metadata need protection (i.e., "time to live").
9. Any additional notes deemed relevant by the agency.

When enumerating cryptographic systems, agencies should keep in mind that an information system or HVA often contains multiple cryptographic systems. They should also note that unused or inactive cryptographic systems should not be included in this inventory. An unused or inactive cryptographic implementation is one that is not, at the time of the agency inventory, actively used for creation and exchange of encryption keys, encrypted connections, or creation and validation of digital signatures.

B. Timelines

Within 30 days of the publication of this memorandum, agencies will designate a cryptographic inventory and migration lead for their organization. Each agency should identify its lead to OMB using the contact information in Section VII. OMB will rely on these designated leads for Government-wide coordination and for engagement on planning and implementation efforts within each organization.

Ninety days after the release of this memorandum, and annually thereafter, ONCD, in coordination with OMB, CISA and the FedRAMP Program Management Office (PMO), will release instructions for the collection and transmission of this inventory, which will include:

- A tool and procedure for agencies to submit their inventory to ONCD and CISA; and
- A process for the identification of common cryptographic systems (e.g., those used by software suites or cloud service providers) used across agencies, so that agencies may avoid inventorying those systems individually.

CISA and the National Security Agency (NSA) will evaluate whether for a security classification guide (SCG) is needed for this inventory. If an SCG is needed, CISA will produce one within 90 days of the issuance of this memorandum.

Agencies can find ONCD's instructions and any related artifacts at the OMB MAX web address provided in Section VII of this memorandum.

III. ASSESSMENT OF FUNDING REQUIRED FOR PQC MIGRATION

No later than 30 days after the submission of each annual inventory of cryptographic systems required under Section II of this memorandum, agencies are required to submit to ONCD and OMB an assessment of the funding required to migrate information systems and assets inventoried under this memorandum to post-quantum cryptography during the following

fiscal year. These agency assessments will inform the funding assessments required by NSM-10 Section 3(c)(iv).

Ninety days after the publication of this memorandum, and annually thereafter, ONCD, in coordination with OMB, will release instructions to agencies that will include:

- A procedure for agencies to submit their funding assessments; and
- A procedure for the collection of funding requirements to migrate common cryptographic systems (e.g., those used by software suites or cloud service providers) used across agencies to simplify and reduce burden of agency cost assessments

Agencies will be able to find these instructions at the OMB MAX web address provided in Section VII of this memorandum.

IV. REPORT ON AUTOMATED CRYPTOGRAPHIC ASSESSMENT PROCESS

Within one year of the publication of this memorandum, CISA, in coordination with NSA and NIST, will release a strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC.

This strategy is expected to address discovery options for internet-accessible information systems or assets, as well as internal discovery of information systems or assets that are not internet-accessible. Discovery methods will support open-source software tools and use existing CISA or agency capabilities, such as Continuous Diagnostics and Mitigation (CDM), where feasible. The strategy will also describe the limitations of available assessment methods, as well as any gaps in automated capabilities or tools.

V. TESTING PRE-STANDARDIZED PQC IN PRODUCTION ENVIRONMENTS

The testing of pre-standardized PQC in agency environments will help to ensure that PQC will work in practice before NIST completes PQC standards and commercial implementations are finalized. Agencies, particularly CISA, are encouraged to work with software vendors to identify candidate environments, hardware, and software for the testing of PQC. Examples of candidate environments, hardware, and software might include web browsers, content delivery networks, cloud service providers, devices and endpoints, and enterprise devices that initiate or terminate encrypted traffic.

To ensure that tests are representative of real-world conditions, they may be conducted, or allowed to operate, in production environments, with appropriate monitoring and safeguards, alongside the use of current approved and validated algorithms. In many cases, the test may be conducted by the vendor across many customers or end users, and agencies are encouraged to participate in these tests.

Within 60 days of the publication of this memorandum, NIST, in coordination with CISA and the FedRAMP PMO, will establish a mechanism, as part of the working group described in

Section VI, to enable the exchange of PQC testing information and best practices among agencies as well as with private sector partners.

VI. CRYPTOGRAPHIC MIGRATION WORKING GROUP

Within 30 days of the publication of this memorandum, OMB and ONCD will establish a cryptographic migration working group consisting of NIST, CISA, NSA, the FedRAMP PMO, and agency representatives. This working group will be chaired by the Federal Chief Information Security Officer and will provide assistance and coordination for agencies conducting cryptographic inventories and migration.

VII. POLICY ASSISTANCE

All questions or inquiries should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: NSM10@omb.eop.gov.

Agencies can find consolidated implementation guidance for this memo on OMB MAX at https://community.max.gov/x/tRBwig.

ATTACHMENTS

APPENDIX A: Interim Benchmarks
APPENDIX B: List of CRQC-Vulnerable Algorithms

APPENDIX A (*as corrected January 8, 2024*)[18]

Interim Benchmarks

Event/Activity	**Actions following publication**	**Responsible Body**
Designate cryptographic inventory and migration lead	Within 30 days	All agencies
Establish a mechanism to enable the exchange of PQC testing information and best practices	Within 60 days	NIST
Release instructions for the collection and transmission of inventory	Within 90 days	ONCD
Release instructions for funding assessments	Within 90 days	ONCD
Release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC	Within 1 year	CISA
Submit cryptographic system inventory	By May 4, 2023 and annually thereafter	All Agencies
Submit funding assessments	30 days after submission of cryptographic system inventory, and annually thereafter	All Agencies
Report testing of pre-standardized PQC	Ongoing	All agencies

APPENDIX B

List of CRQC-Vulnerable Algorithms

Algorithm	**Function**	**Specification**
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Menezes-Qu-Vanstone (MQV) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithms used for digital signatures	FIPS PUB 186-4
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526
RSA Signature Algorithm	Asymmetric algorithm used for key establishment	FIPS SP 800-56B Rev. 1

[18] The "Responsible Body" for the "Submit cryptographic system inventory" and "Submit funding assessments" requirements has been corrected to reflect that these requirements apply to all agencies, although they do not apply to national security systems.

Digital Signature Algorithm	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4
Other non-PQC Asymmetric Algorithm[19]	Remaining asymmetric algorithms not enumerated in the list above	Not applicable

[19] Agencies should work with CISA and vendors of products that utilize asymmetric algorithms not enumerated in this table to determine if these algorithms are quantum-vulnerable. Agencies are encouraged to include any asymmetric algorithm that is not definitively known to be quantum-resistant.