U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Issue Date: 09/17/2021
Expiration Date: (two years after issued date)

Policy Directive 140-15

MEMORANDUM FOR: Distribution

FROM: Eric Hysen
Chief Information Officer

SUBJECT: Preparing for Post-Quantum Cryptography

Purpose: DHS has significant national security concerns across mission spaces including critical infrastructure, law enforcement, privacy, and counterintelligence that could be harmed by insufficient preparation for a transition to post-quantum cryptography. This memorandum provides guidance to Component Heads to begin preparing for a transition from current cryptography standards to post-quantum encryption now to mitigate risks to data and mission functions.

This memorandum provides Component Heads with an overview of some specific risks to the DHS mission, and a roadmap to take action against the quantum threat to current cryptographic systems. While there is no U.S. Government-approved post-quantum cryptographic standard as of the release of this Statement, these preparatory steps will significantly reduce the time required for transition once industry adopted and U.S. Government validated algorithms are available, resulting in continued mission success and a more secure homeland.

The threat posed to current cryptographic methods extends beyond the Department, affecting interagency, international, and private sectors partnerships critical to mission success. The roadmap below should be used by Components to encourage effective and consistent transition preparation among DHS partners. The potential costs of a slow or ineffective transition to post-quantum cryptography present significant threats to DHS operations and the security of the homeland and must be addressed in a cooperative manner. DHS is prepared to take a leadership role in pursuit of a secure homeland and continued mission success.

Background: Cryptographic technologies are used throughout the Department of Homeland Security (DHS) to authenticate the source and protect the confidentiality and integrity of communicated and stored information. Cryptography is used to secure information relating to law enforcement, immigration, border security, trade regulation, critical infrastructure security, incident response, research and development, and other critical mission areas.

DHS uses symmetric and asymmetric cryptographic algorithms to secure sensitive data and protect secure communications across the homeland security mission space. With the use of cryptographic technologies comes the responsibility to monitor those systems for weakness,

constraints imposed by dependent technologies, or advances in the technologies that support cryptanalysis to determine when replacement is necessary.

Advances in quantum information science (QIS) present a significant advance in current cryptanalytic capabilities, which poses a threat to conventional public-key cryptographic systems relied upon by the government and private sector alike, should an adversary achieve a practical quantum computer.

Due to the broad use of asymmetric cryptography across diverse and interconnected systems, a transition from current cryptographic technologies to a post-quantum algorithm could take years to complete. The rapid pace of technological advancement over the years required for transitioning systems to the new cryptographic standard could create new vulnerabilities and result in a repeating cycle. It is, therefore, of critical importance that DHS begin preparation for post-quantum encryption now by taking some initial steps and by understanding the risk of QIS-enabled cryptanalysis.

Specifically, the cryptographic systems Rivest, Shamir, Adleman (RSA), Elliptical Curve Cryptography (ECC), and Diffie-Hellman key exchange will eventually have their public keys compromised by a quantum computer capable of running Shor's Algorithm. Further, symmetric cryptographic algorithm, Advanced Encryption Standard (AES) with a 128-bit key size is vulnerable to Grover's Algorithm and can be compromised with the assistance of quantum computing. Use of longer key lengths may mitigate some risk depending on the pace and cost of quantum technology evolution. Components should begin planning for replacement of quantum-vulnerable products with quantum-resistant products as soon as standardization, implementation, and testing of replacement products using the newly approved algorithms are complete, consistent with applicable rules and processes governing data and system security. Components will identify the data that need to be protected and its associated length of time to remain so. Components will identify and submit existing cryptographic technology inventories and plans for transition to the DHS Office of the Chief Information Officer (OCIO) per the below roadmap outlined in this statement.

Roadmap: The risks to current cryptographic technologies that enable DHS mission activities and the need for action to protect them are clear. However, quick action without the necessary preparations will result in an inconsistent and disjointed response to post-quantum encryption comprised of siloed individual cryptography transitions that will come at a significant cost to Department resources and readiness.

In partnership with the National Institute of Standards and Technology (NIST), DHS developed the below roadmap to provide Component Heads with a realistic path to address post-quantum encryption on a timeline that matches the production of a new government-wide post-quantum encryption standard, likely to be published as early as 2024.

Previous transitions to new cryptographic standards have taken between 5 and 15 years to complete given the breadth of the standard's use. The current pace of QIS technology development combined with an incomplete understanding of QIS's full implications, creates a convergence that may result in new cryptanalysis tools coming available before the new post-quantum standards are fully in place.

A slow transition could prove costly in terms of security and resources making preparation critically important. While the exact timeline of a quantum computer capable of executing advanced algorithms putting DHS cryptographic equipment inventory at risk is uncertain, the significance of the risk is not. Building quantum resilience within the Department is a critical need for which proactive planning and preparation are required. Understanding the threat to specific mission areas and developing solutions based on mission need using the below roadmap will result in a more secure Department and nation for decades to come.

Components shall not procure any post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST.

Plans for transition and cryptographic technology inventories are key elements to the Department's overall quantum preparedness. The DHS Chief Information Security Officer (CISO) will provide guidance to components for conducting cryptographic technology inventories not later than the third quarter of Fiscal Year (FY) 22 and establishing plans for transition not later than the first quarter of FY 23. DHS OCIO will provide additional guidance to components after inventories and transition plans are submitted, to align with NIST establishing standards.

A) **Standards Developing Organization Outreach**: Component Heads should direct their CIOs to increase their engagement with standards developing organizations (SDOs) to raise awareness of necessary algorithm and dependent protocol changes. This early engagement will reflect the Department's prioritization of this issue and position it to be an active participant in policy and technical discussions about required changes in its systems.

B) **Inventory Critical Data**: Components shall inventory their most sensitive and critical datasets that must be secured for an extended amount of time. This information will inform future risk analysis by identifying what data may be stolen now and decrypted once a sufficient quantum computer is available.

C) **Inventory of Cryptographic Technologies**: Components will conduct an inventory of all the systems using cryptographic technologies for any mission function.

D) **Identify Internal Standards**: The DHS CISO will identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

E) **Identification of Public Key Cryptography**: From the inventory, Components should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

F) **Prioritize Systems for Replacement**: Prioritizing one system over another for cryptographic transition is highly Component-dependent and should be based on mission requirements. To supplement prioritization efforts, Components shall consider the following factors when evaluating a quantum vulnerable system:

1. Is the system a high value asset based on mission requirements?

2. What is the system protecting (e.g., key stores, passwords, root keys, signing keys, personally identifiable information (PII), sensitive personally identifiable information (SPII))?

3. What other systems does it communicate with?

4. To what extent does the system share information with other federal entities?

5. To what extent does the system share information with private sector entities?

6. Does the system support critical infrastructure?

7. How long does the data need to be protected?

G) **Plan for Transition**: Using the inventory and prioritization information, Components shall develop a plan for system transitions consistent with mission requirements upon publication of the new post-quantum cryptographic standard. DHS CISO will provide guidance for creating transition plans.

References:

Barker, Polk, and Souppaya, *Getting Ready for Post-Quantum Cryptography*; National Institute of Standards and Technology, U.S. Department of Commerce; May 26, 2020.

Executive Order 13885, *Establishing the National Quantum Initiative Advisory Committee* (Signed August 30, 2019)

U.S. Cyberspace Solarium Commission, *Solarium Commission Report, Recommendation 6.2.4* (March 2020)