OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

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

b. What is the system protecting (e.g. key stores, passwords, root keys, singing keys, personally identifiable information, sensitive personally identifiable information)?

c. What other systems does the system communicate with?

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

e. To what extent does the system share information with other entities outside of your organization?

f. Does the system support a critical infrastructure sector?

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

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.

2021-2023
Inventory and prioritize systems

2024
NIST post-quantum cryptography standard published

2024-2030
Transition of systems to NIST post-quantum cryptography standard

2030
Cryptographically relevant quantum computer potentially available