Chairman Jay Obernolte

Securing the Nation Against Advanced Cryptographic Attacks

Administration Policy:

On June 23rd, 2026, the White House issued an Executive Order to help secure the nation against advanced cryptographic attacks. The White House factsheet is available here.

The EO warns that advances in quantum computing may eventually allow adversaries to break the encryption systems currently used to protect government data, critical infrastructure, and the digital economy. It also points out that foreign actors may already be collecting encrypted information today with the intention of decrypting it once powerful quantum computers become available. The EO assigns overall responsibility for coordinating the federal transition to post-quantum cryptography (PQC) to the Office of Management and Budget (OMB) and the National Cyber Director. The National Institute of Standards and Technology (NIST), working with the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), is directed to provide technical guidance and implementation support.

To accelerate adoption, agencies must designate a Post-Quantum Cryptography Migration Lead within 30 days. Within 90 days, OMB must issue guidance to federal agencies that requires them to identify high-value assets and high-impact systems, including a plan for agencies to transition such assets and systems to PQC-based key establishment technologies. NIST is also directed to launch a pilot program demonstrating PQC implementation on selected systems by the end of 2027.

Beyond the federal government, the EO directs Sector Risk Management Agencies and CISA to assist critical infrastructure operators in developing PQC migration plans. The Department of State is tasked with encouraging foreign governments and industry groups to adopt NIST-standardized PQC technologies. The EO also asks federal agencies to promote joint procurement of technology, share technical expertise, move systems to secure cloud environments, and participate in joint training programs to reduce costs and improve efficiency.

Furthermore, the EO directs NIST to simplify and speed up the approval process for encryption products so that new technologies can be deployed more quickly. Finally, the EO directs the Federal Acquisition Regulatory Council to propose regulations requiring federal contractors to comply with NIST PQC standards by December 31, 2030, and to strengthen contractor vulnerability disclosure requirements for cryptographic weaknesses and outdated encryption technologies.

Background:

- The National Cyber Director serves as the principal advisor to the President on cybersecurity policy and strategy and was established by Section 1752 of the FY2021 National Defense Authorization Act (Public Law 116-283; 6 U.S.C. § 1500).
- According to NIST, post-quantum cryptography (PQC) is a new generation of encryption designed to protect data from future quantum computers, which could be powerful enough to break many of the encryption methods that secure government systems, financial transactions, and private communications today.
- NIST also notes that although adversaries cannot crack encryption now, adversaries may benefit from capturing encrypted data now and holding on to it in hopes that a quantum computer will break its encryption in the future, an idea sometimes expressed as “harvest now, decrypt later.”