Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Preparing Secrets for a Post-Quantum World—National Security Memorandum 10

May 9, 2022

On May 4, 2022, President Biden signed National Security Memorandum 10 (NSM 10) on *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.* Along with an accompanying Executive Order (EO), the memorandum seeks to promote U.S. leadership in quantum information science (QIS). NSM 10 also addresses potential threats that quantum computers may pose to encrypted data and systems.

This Insight discusses the cybersecurity risks posed by quantum computing, details about the memorandum, and potential issues for Congress.

Encryption

Encryption uses the art of cryptography to change information which can be read (plaintext) so that it cannot be read (ciphertext). Cryptography is used to protect the confidentiality and integrity of sensitive documents, data stores, and systems (e.g., critical infrastructure). Encryption is also used to secure identities, create unique identifiers to authenticate data, and enable blockchain-based technologies.

Size and Security

Many federal and commercial information technology (IT) systems use the Advanced Encryption Standard (AES). AES keys are in lengths of 128, 192, and 258 bits (i.e., size). One may also express a 128-bit key as 2^{128} bits. If an attacker wanted to access data encrypted by an AES-128 key, they would need to guess each possible combination of the key. They would, on average, discover the key after running through half the options (i.e., 2^{127} tries). Using a single, modern computer, this attack would take longer than the age of the universe to complete. Attackers tune their algorithms to reduce the possibilities of passwords, thereby greatly increasing their likelihood of success. Knowing the conditions of a password (e.g., complexity requirements) would further reduce the available options to try. For example, short or numerical passwords may only take days to discover.

Congressional Research Service
https://crsreports.congress.gov
IN11921

Risks from Quantum Computing

Today's classical computers process operations by manipulating binary bits (1 or 0). Quantum computers take advantage of superposition and entanglement of bits to significantly speed up operations, which would reduce the time necessary to discover an encryption key. Current quantum computers are in a nascent state of development and are not known to be capable of conducting enough sustained operations to pose a threat to AES keys. But ongoing research could lead to quantum computers that are capable of such operations. If that happens, cryptanalysts with access to quantum computers will be able to discover keys exponentially faster—for instance, 2^{64} tries for an AES-128 key. A mathematician has already developed the algorithm to break today's encryption with quantum computers.

Given this potential, cybersecurity experts are concerned about steal-now and decrypt-later attacks whereby nation-state actors download encrypted data from the U.S. government and critical infrastructure operators today with the hopes of using quantum computers to decrypt that data at some point in the future. Additionally, systems that continue to use current encryption standards in a future with cryptanalytically relevant quantum computers will immediately risk having their security compromised.

Anticipating this shift, the National Institute of Standards and Technology (NIST) has initiated a project on quantum-resilient cryptographic (QRC) standards.

NSM 10

NSM 10 requires the federal government to partner with the private sector on developing and adopting QRC standards, and develop plans to transition to them. To assist non-federal entities, the Cybersecurity and Infrastructure Security Agency (CISA) is to work with sector risk management agencies (SRMAs) and engage with state and local governments, as well as the private sector, to educate them on the risks to encryption from quantum computing.

Table 1 lists NSM 10 requirements for federal agency QRC adoption.

Table 1. NSM Requirements for Federal Agency IT

Action	Agencies	Deadline
Create public-private working group to advance and adopt QRC.	NIST	8/2/22
Create a dedicated project to work with the private sector to transition to QRC.	NIST	8/2/22
Set requirements to inventory cryptosystems used by agencies.	OMB	10/31/22
Report on systems that remain vulnerable to attacks on encrypted data from quantum computers.	All agencies to CISA and NCD	5/4/23 and annually thereafter
Issue guidance for QRC and National Security Systems.	NSA	5/4/23
Report to OMB on the status of agency QRC transitions and recommendations on funding needed to facilitate transition.	NCD	10/18/23 and annually thereafter
Propose a timeline for the deprecation of quantum-vulnerable cryptographic standards.	NIST	Within 90 days of the release of QRC standards (expected 2024)
Set requirements to develop plans to transition quantum-vulnerable systems to QRC.	OMB	A year after NIST publishes standards

Source: CRS analysis of NSM 10.

Notes: Office of Management and Budget (OMB). National Cyber Director (NCD). National Security Agency (NSA).

The NSA is to manage similar QRC transition efforts for national security systems, with deadlines similar to those for civilian systems.

Issues for Congress

As entities continue to develop QRC and transition to those standards, Congress may choose to engage in those developments—as it has recently done with the United States innovation and competition legislation, which includes funding and authorities for QIS workforce and QRC development.

NSM 10 creates a new requirement for federal agencies. Adding QRC transitions to existing EO 14028 cybersecurity requirements (e.g., migration to zero trust architecture, or ZTA) reflects a significant shift in how agencies design, build, and operate their networks. Ensuring adequate plans, contracts, and deployment of future IT systems will require resources not currently budgeted. The President's FY2023 Budget has requests for ZTA transition, but only includes references to a QIS-ready workforce, not QRC transition planning.

The Government Accountability Office (GAO) has found that while the federal government makes efforts to share cybersecurity risk information with the private sector, it has not assessed the effectiveness of its efforts. Given the scope and scale of present-day encryption deployment, CISA would likely need to develop new communication strategies in order to reach and educate entities nationwide on this risk.

As activity around international QRC standards development increases, agencies will likely need to refocus staff and resources to support those efforts. NIST is requesting a $15 million increase to support QIS efforts, and the Department of State is requesting a $1.9 million increase to support the new Special Envoy for Emerging and Critical Technology.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer