White House drastically shortens deadline for dropping quantum-vulnerable crypto

The White House is drastically shortening the deadline for government agencies and organizations to adopt new quantum-resistant encryption systems that will withstand attacks that use quantum computers, as the federal government seeks to protect decades' worth of secrets belonging to militaries, banks, governments, and most individuals on Earth.

The executive order, titled Securing the Nation against Advanced Cryptographic Attacks, requires computing systems for "high-value assets" and "high-impact systems" to transition to post-quantum cryptographic key establishment schemes by December 31, 2030, and to quantum-safe digital signature schemes by December 31, 2031.

Heading off a significant threat

The new deadline, which for many organizations is about five years sooner than the previous one, comes on the heels of recent research showing that the resources and cost for building a cryptographically relevant quantum computer are far less than previous consensus estimates. In response, Google, Cloudflare, and other companies recently tightened their timelines for moving off vulnerable systems to 2029.

"The advent of large-scale quantum computers, particularly in the hands of adversaries, will pose a significant threat to

widely used cryptographic security systems," Monday's executive order stated. "Ongoing cyber activity against our Nation also presents the risk of adversaries collecting United States information now, and decrypting it later once large-scale quantum computers are operational."

Under a timeline the National Security Agency published in 2022, "National Security Systems"—a class including only defense and intelligence systems under the authority of the agency—were under orders to be quantum-ready between 2030 and 2033. Most other organizations had until 2035 to complete the transition. Now, many of them will be required to transition much sooner.

"So, for any system that falls into this new bucket of high-value assets and high-impact systems, their transition timelines just got shortened by 4-5 years (from 2035 to 2030/2031)," Brian LaMacchia, a cryptography engineer who oversaw Microsoft's post-quantum transition from 2015 to 2022 and now works at Farcaster Consulting Group, told Ars. "That is a significant shortening of the transition timeline for these systems, and it follows similar timeline revisions from Google and Cloudflare that we saw announced back in late March/early April."

https://arstechnica.com/information-technology/2026/06/executive-order-bumps-up-deadline-to-move-off-quantum-vulnerable-crypto/