NSM-8: Government Mandates Quantum Resistant Cryptography for Protecting Federal Networks

The Biden White House is serious about cybersecurity and its zero-trust agenda, releasing NSM-8, a memorandum on "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." This builds on the original Executive Order 14028 issued on May 12, 2021 to improve the nation's cybersecurity and protect federal government networks. NSM-8 sets forth new requirements that are equivalent to, or exceeds, the cybersecurity requirements within Executive Order 14028 including an emphasis on quantum-resistant cryptography for federal cybersecurity planning.

If you follow Quantum Xchange then you know we've been encouraging federal agencies and their partners to embrace quantum-safe encryption as part of the original EO for Improving the Nation's Cybersecurity, believing that sections 3.d and 3.c didn't go far enough in its recommendations for encrypting data in transit or prioritizing the most sensitive data under the greatest threat. See our blog post, Countdown to Encryption: Only 120 Days Remain for Meeting the White House Executive Order on Encrypting Data in Motion and expert article appearing in Government Computer News, "Why Quantum and Data Protection Should Go Hand-in-Hand."

Seems the White House agrees. The NSM-8 memorandum instructs the NSA to share with agency CIOs any relevant documents related to "quantum resistant protocols, and planning for use of quantum-resistant cryptography where necessary."

The provision states verbatim: Within 180-days of the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI//NOFORN.

NSM-8 is a big win for those like Quantum Xchange and other members of the Quantum Alliance Initiative, who have been championing the federal government to take the quantum threat seriously as a cybersecurity priority since 2018.

Federal agencies and their integration partners looking to meet the NSM-8 180-day mandate, should consider Phio TX from Quantum Xchange. The next-generation key delivery system meets the NSA's quantum resistant key distribution protocol as outlined in "Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex V2.0 (January 2021)" by using pre-shared keys in the Phio TX hive and featuring the ability to automate pre-shared key rotation for system users. Phio TX also features all Post-Quantum Cryptographic (PQC) key encapsulation algorithms being evaluated by NIST with final selection expected for release in early 2022. Visit the Quantum Xchange Government Resource Center for more information.

But what about the private sector?

As our friend and colleague Arthur Herman so eloquently points out in his recent *Forbes* column, "Given the fact that the federal government finally admits this is a security threat grave enough to demand action from agencies within the next 180-days, that's all the more reason why private industry needs to take this threat seriously, without waiting for the slow-moving bureaucratic machinery of Washington to put together a plan to protect the rest of us."

There's too much at stake not to act now and as Mr. Herman shares, "there are right now safe ways to protect data networks from future quantum intrusion but also existing cyber attackers…there's no reason to wait until the NSA or the NIST make their final section of quantum-resistant algorithms, and federal agencies finally respond."

Phio TX from Quantum Xchange is one of those "right now" quantum-safe solutions. Contact us today to learn more.