The U.S. Just Set an Aggressive Post-Quantum Deadline, and Its Reach Extends Far Beyond American Borders

Securosys Confirms Its HSMs Support NIST-Certified PQC Algorithms and Launches PQC Sandbox for Migration Testing

The Securosys management team. From the left: Andreas Curiger (CTO/CSO), Robert Rogenmoser (CEO), Marcel Dasen (Executive VP Engineering), Reto Stäuble (Executive VP Solutions & Services), and Pal Blasko (CFO).

ZURICH, SWITZERLAND, July 16, 2026 /EINPresswire.com/ -- Securosys SA, a Swiss leader in cybersecurity, cloud security, encryption technology, and digital identity protection, today confirmed that its hardware security modules (HSMs) already support the post-quantum cryptography (PQC) algorithms standardized by NIST, a capability that international organizations doing business with the United States may need sooner than they think.

On June 22, 2026, President Donald J. Trump signed Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks." The order requires U.S. federal agencies to transition high-value assets and high-impact systems to PQC for key establishment by December 31, 2030, and to PQC for digital signatures by December 31, 2031.

But the order's provisions do not stop at U.S. federal agencies. Within 180 days, the Federal Acquisition Regulatory Council (FAR Council) must publish a proposed rule requiring covered government contractors to comply, by December 31, 2030, with NIST's FIPS standards, including those incorporating PQC-compliant algorithms. The order also directs the Secretary of State, working alongside NIST, the Department of Homeland Security, the National Cyber Director, the Department of War, and the Director of National Intelligence, to reach out to foreign governments and industry groups in key countries and encourage them to adopt NIST-standardized PQC algorithms.

What This Means Outside the U.S.

For organizations headquartered in Europe, Asia, or elsewhere, Executive Order 14412 is not a domestic U.S. policy document to file away. Any organization that supplies technology or services to U.S. government agencies, directly or through its supply chain, falls within the scope of the FAR Council's forthcoming contractor requirement. Separately, the order commits the U.S. government to actively engaging foreign governments and industry groups to encourage adoption of NIST-standardized PQC algorithms abroad.

In summary: Executive Order 14412 sets an aggressive post-quantum timeline for U.S. federal agencies, and its contractor and foreign-engagement provisions extend its effects to international tech suppliers, cloud providers, and any global firm doing business with the U.S. Waiting for local regulation to catch up is no longer a safe strategy. Migration starts now.

CEO Statement

Robert Rogenmoser, CEO of Securosys, said:

“Executive Order 14412 was written for U.S. federal agencies, but it doesn't stop there. It puts a concrete requirement on government contractors, and directs the Secretary of State to actively engage foreign governments and industry groups to encourage their adoption of the same NIST-standardized PQC algorithms. Any company that supplies technology to the U.S. government, directly or through its supply chain, should take note. We've been preparing our HSMs for exactly this moment, and organizations anywhere in the world can start validating their own PQC migration today.”

Your HSM Plays a Key Role in the PQC Transition

Securosys has been preparing for this transition by integrating NIST-standardized post-quantum algorithms into its FIPS 140-3 Level 3 compliant HSM portfolio and supporting hybrid cryptographic approaches designed for a gradual migration. An organization's HSM plays a central role in this process: it can be used to test new cryptographic operations, validate application compatibility, support hybrid cryptographic deployments during the transition period, and prepare for the larger keys and signatures required by PQC algorithms. The path runs from current applications, through hybrid cryptography, to fully PQC-ready infrastructure.

To support this, the Securosys CloudHSM Sandbox can be used to validate a migration strategy before production, allowing organizations to experiment with NIST-standardized PQC algorithms — including ML-KEM, ML-DSA, SLH-DSA, HSS-LMS, and XMSS — in a secure, fully managed environment designed specifically for development and integration testing. The Sandbox is designed to help teams move from evaluation to implementation with confidence, and includes:

- NIST-standardized PQC algorithms
- Industry-standard APIs: REST, PKCS#11, JCE, and Microsoft CNG
- Engineering support, including access to detailed debug logs and direct collaboration with Securosys engineers

Securosys is offering free, limited-time access to the PQC Sandbox as a proof of concept, with immediate access and no production risk.
For more information, please visit the Securosys website.

Martina Alig
Securosys SA
+41 44 552 31 00
email us here
Visit us on social media:
LinkedIn
