The White House Accelerates PQC Transition: Securosys HSMs Already Support NIST-Certified PQC Algorithms

Securosys Confirms Its HSMs Already Support NIST-Standardized PQC Algorithms and Launches Free 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, 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. The confirmation follows the signing of Executive Order 14412 by President Donald J. Trump on June 22, 2026.

The United States is accelerating its transition to post-quantum cryptography. With Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," the White House has established an accelerated timeline for migrating federal information systems to quantum-resistant cryptography. The order highlights the growing risk that adversaries could collect encrypted information today and decrypt it in the future once large-scale quantum computers become available. It also defines a policy to transition federal information systems to NIST-approved Federal Information Processing Standards (FIPS) for post-quantum cryptography (PQC) while supporting critical infrastructure owners and operators in their own migrations. The order introduces ambitious timelines for protecting high-value assets with quantum-resistant cryptography and calls for faster certification of cryptographic modules.

What Executive Order 14412 Requires

According to the order, agencies must transition all high-value assets (HVAs) and high-impact systems to PQC for key establishment by December 31, 2030, and to PQC for digital signatures

by December 31, 2031. Within 180 days, NIST is required to revise the Cryptographic Module Validation Program (CMVP) validation processes to accelerate the certification of cryptographic modules. During the same period, the Federal Acquisition Regulatory Council (FAR Council) must propose new procurement rules requiring covered contractors to comply with applicable NIST FIPS standards, including those incorporating NIST-standardized PQC algorithms, by December 31, 2030.

In summary: The Executive Order accelerates the adoption of post-quantum cryptography (PQC) for high-value assets and calls for faster certification of cryptographic modules. For organizations protecting long-lived sensitive data, PQC migration is moving from future planning to active implementation. Migration starts now.

CEO Statement
Robert Rogenmoser, CEO of Securosys, said:
“Every day sensitive data is encrypted with classical algorithms is a day it can be harvested and decrypted later once quantum computers catch up. Executive Order 14412 puts a hard deadline on that risk for federal high-value assets. We've been preparing our HSMs for exactly this moment, and our message to organizations managing long-lived sensitive data is simple: don't wait for the compliance deadline to force your hand; start testing your PQC migration now.”

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 the PQC Sandbox free of charge for three months, 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
