![SafeLogic logo] **SafeLogic**

carahsoft.

Federal Government Suppliers Mandated to Support PQC

Thank you for downloading this SafeLogic datasheet. Carahsoft is the master government aggregator and distributor for SafeLogic's Cybersecurity solutions available via NASA SEWP V, ITES-SW2, NASPO ValuePoint and other contract vehicles.

To learn how to take the next step toward acquiring SafeLogic solutions, please check out the following resources and information:

For more information:
carah.io/SafeLogic

For upcoming events:
carah.io/SafeLogicEvents

To set up a meeting:
SafeLogic@carahsoft.com
844-214-4790

For additional resources:
carah.io/SafeLogicResources

Federal Government Suppliers
Mandated to Support PQC

On June 6, 2025, the **President issued Executive Order 14306, "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144,"** directing federal agencies to **bolster cybersecurity against emerging threats, including quantum computing risks** requiring the Department of Homeland Security, through CISA and in consultation with the NSA, to publish and regularly update a list of product categories in which post-quantum cryptography (PQC)-capable products are widely available.

In response**, CISA released its Product Categories for Technologies That Use Post-Quantum Cryptography Standards list**, identifying hardware and software categories — such as cloud services, web software, networking, and endpoint security — where PQC standards are implemented or maturing, and advising organizations to prioritize PQC-capable products in acquisition planning to future-proof security and manage the transition to quantum-resilient cryptography.

> "When a particular category offers widely available PQC-capable products, organizations should plan acquisitions to procure only PQC-capable products from that category."

SafeLogic is Your
Strategic Cryptography Software Partner

SafeLogic delivers the fastest and easiest way to qualify your products to meet the PQC standards for products that are now considered "widely available" by CISA.

SafeLogic CryptoComply is a family of FIPS 140-3 validated, 'drop-in compatible' cryptographic software that **enable your products with full NIST standard PQC algorithm support**, NIST validated entropy sources, crypto-agility, and classical encryption with Enterprise-level support.

PQC algorithms: ML-KEM (FIPS 203),
ML-DSA (FIPS 204), and SLH-DSA (FIPS 205)
Hybrid mode key exchange: combines SafeLogic's FIPS 140-3 certified classical algorithms with ML-KEM
API compatibility: OpenSSL, Bouncy Castle
OS support: Android, iOS, Linux, MacOS, Unix and Windows
Programming languages: C, C++, Go, Java, Python, Rust and more
Deployment models: Cloud, containers, appliances, embedded, and IoT systems

Learn more:

- **[CISA: Product Categories for Technologies That Use Post-Quantum Cryptography Standards](#)**
- **[CISA: Widely Available Hardware and Software Product Categories That Use PQC Standards](#)**
- **[SafeLogic: CryptoComply Cryptography Software](#)**