National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

NIAP Policy Letter #33

31 August 2026

SUBJECT: Post Quantum Cryptography Implementation.

REFERENCES:
Committee on National Security Systems Policy No. 15, "Use of Public Standards for Secure Information Sharing" March 2025

Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, Version 2.1, December 2024

Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks" June 2026

National Security Presidential Memorandum/NSPM-12, June 2026

PURPOSE: This policy establishes the timeline for implementation of Post Quantum Cryptography (PQC) requirements.

BACKGROUND: Placement on the NIAP Product Compliant List (PCL) makes a product eligible for procurement for use in National Security Systems (NSS). Introduced in 2016, Annex B of the Committee on National Security Systems (CNSS) Policy (CNSSP) No. 15 defines the Commercial National Security Algorithm (CNSA) Suite 1.0, which mandates cryptographic algorithms meeting acceptable minimum standards for use in NSS. Introduced in 2022 and formalized in 2025, CNSA 2.0 mandates use of cryptographic algorithms meeting PQC requirements for use in NSS. NSPM-12 re-establishes the CNSS and affirms that CNSSP 15 constitutes the commercial cryptographic standard for NSS.

Beginning 1 January 2027, government contracts must include language requiring products used in NSS implement PQC or be updateable to implement PQC. To meet the CNSA and EO 14412 timelines while being realistic about the widespread use of non-CNSA algorithms in functions like secure boot and trusted update, NIAP requires a PQC policy with clear timelines.

POLICY: Products submitted to NIAP for evaluation which meet all CNSA 2.0 requirements will be prioritized for validation resources over products which do not fully comply with CNSA 2.0. Products which partially meet CNSA 2.0 requirements will be prioritized for validation resources over products which do not comply at all with CNSA 2.0.

To ensure that NIAP certifications beginning in 2027 are enabling the transition to CNSA 2.0 and quantum resistance, products (certified by either NIAP or a CCRA partner) which do not meet CNSA 1.0 minimum requirements for every cryptographic function have the following restrictions:

- are no longer eligible for extending certificate length via Assurance Maintenance;
- cannot have a certificate length over two years, regardless of certificate length outlined in Policy #29;
- will not be accepted by NIAP into evaluation beginning 1 January 2027;
- will not be posted to the NIAP PCL beginning 1 July 2027;
- will be archived at a date to be determined, regardless of time remaining on their certification.

Products (certified by either NIAP or a CCRA partner) which do not meet CNSA 2.0 requirements for

every cryptographic function have the following restrictions:

- will not be accepted by NIAP into evaluation beginning 1 January 2028;
- will not be posted to the NIAP PCL beginning 1 January 2029;
- will be archived at a date to be determined, regardless of time remaining on their certification.

Use of AES-128 for Bluetooth will be the exception to this policy until the Bluetooth standard is updated.

EFFECTIVE DATE: This policy is effective 1 January 2027.

Original Signed By

Marcus Parker
Director, NIAP

9800 Savage Road, STE 6940, Ft. Meade, MD 20755-6940
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: niap@niap-ccevs.org
http://www.niap ccevs.org/