U.S. AIR FORCE

C3I and Networks Directorate



Next-Gen Cryptography: Securing Enterprise Infrastructure

Anthony Bellavia
Section Chief, Cryptography & Credentials
PM, Public Key Infrastructure (PKI)
AFLCMC/HNID

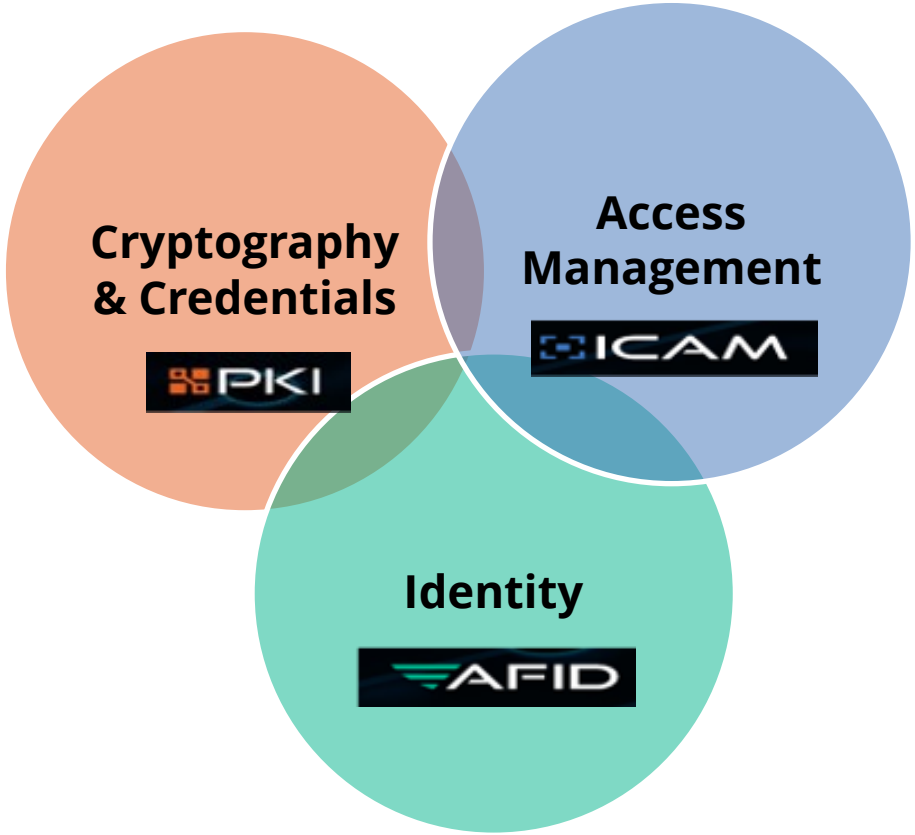
DISTRIBUTION STATEMENT A. Approved for public release (5 AUG 2026); distribution is unlimited.

HNID: Identity Solutions Branch

- The Air Force Life Cycle Management Center (AFLCMC) Identity Solutions Branch (HNID) is responsible for acquiring, developing and delivering capabilities to secure cyberspace through robust Identity, Credential, Access Management (ICAM), Public Key Infrastructure (PKI) solutions and Air Force Identity.

- Our core mission is to ensure secure, uninterrupted authentication and authorization to systems, data, and information.

- HNID is your partner in cyber defense. Whether you are a Wing Cybersecurity Liaison, a System Owner, or a Program Manager, our team is here to provide the tools, guidance, and cryptographic infrastructure needed to secure your systems and protect our warfighters.



The Fundamentals of Identity Solutions

U.S. AIR FORCE

IDENTITY

1

Ensure **identity and attribute information** is accurate and accessible for mission requirements

CREDENTIAL

2

Develop, deliver and sustain **cryptographically assured credentials**

ACCESS

3

Secure managed access to mission-specific applications, tools and systems

Priorities:

Enable Joint Force Interoperability: Standardizing identity assurance levels to allow seamless, secure collaboration across joint and coalition networks.

AFID

Modernize PKI & Cryptography: Driving the transition to next-generation algorithms (CNSA 1.0) and preparing the DAF for the Post-Quantum Cryptography (CNSA 2.0) threat landscape.

PKI

Operationalize Zero Trust: Delivering the cryptographic and identity foundations required to achieve absolute data security across multi-domain operations.

ICAM

U.S. AIR FORCE

Agenda

- Executive Summary
- PKI and the Quantum Threat
- Mandates and Policies
- Algorithm Evolution (CNSA 1.0)
- PQC Migration (CNSA 2.0)
- Cryptographic Inventory
- Take Action



Executive Summary

The Threat

Quantum computing will soon compromise traditional asymmetric encryption.

The Algorithm Evolution Mandate (CNSA 1.0)

The ongoing deployment of stronger PKI utilizing larger key sizes until quantum resistant algorithms can be fully implemented.

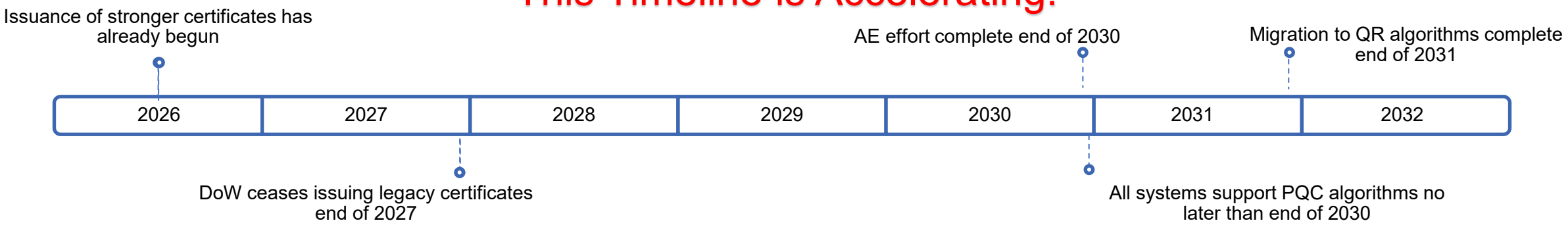
The Post-Quantum Mandate (CNSA 2.0)

Transition all DoD and National Security Systems to quantum-resistant cryptography.

Your Mission

Inventory systems, identify gaps, prepare for timeline acceleration, and execute the transitions.

This Timeline is Accelerating!



PKI Background – The Framework of Trust

- Public Key Infrastructure (PKI) is a framework that is established to issue, maintain, and revoke public key certificates[1]
- Built on asymmetric cryptography
- Binds keys to identities to establish trust

Capability	What does that mean?
Confidentiality	Encrypts data to protect it from unauthorized viewing
Data Integrity	Ensures information has not been altered or tampered with in transit
Non-Repudiation	Provides undeniable cryptographic proof of origin
Authentication	Validates identities before granting network or data access

[1] National Institute for Standards and Technology

The Quantum Threat

- Cryptographically Relevant Quantum Computers (CRQC) threaten PKI
- The Threat Today: "Harvest Now, Decrypt Later" (HNDL)
- The Threat Tomorrow: Cryptographic Obsolescence
- The Solution: Continue to deploy Algorithm Evolution (AE) now and transition to Post Quantum Cryptography (PQC) to secure the future.

U.S. AIR FORCE

Mandates and Policies

Directive/Standard	Mandate and Impact
NSA CNSA 1.0	Requires scaling traditional algorithms to larger key sizes. (RSA 4096/3072 and SHA-384)
NSM-8, NSM-10 & OMB M-23-02	Mandates NSS achieve quantum resistance by 2035; requires annual vulnerability reporting and cryptographic inventories
NSA CNSA 2.0	Mandates the complete transition away from traditional PKI to quantum resistant algorithms. (FIPS-203 ML-KEM, FIPS-204 ML-DSA)
CNSSP 11 & CNSSP 15	Deprecates CNSA 1.0, revokes previous waivers, and ties commercial NIAP validation to CNSA 2.0 compliance
DAF CIO Memo Feb 26, 2026	Aligns DAF with CSWP-48 and formally adds PQC transition requirements into the Risk Management Framework (RMF)
DoW CIO Memo April 01, 2026	Accelerates PQC timelines for systems to support PQC by end of 2030 and mandates exclusive use by end of 2031

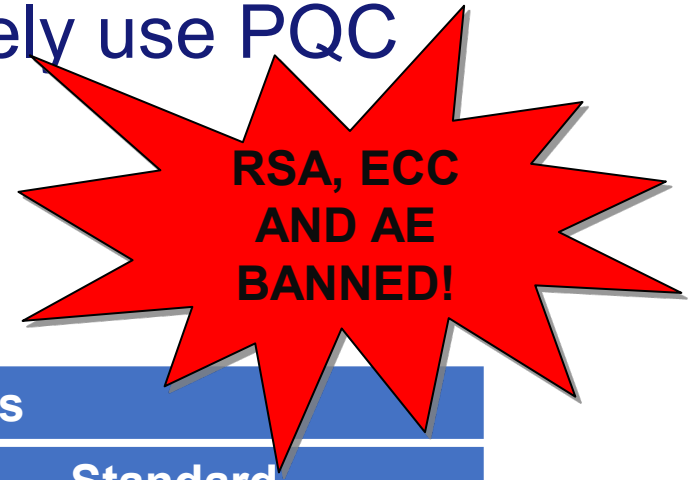
U.S. AIR FORCE

Algorithm Evolution – CNSA 1.0

What is the Algorithm Evolution?	• Ongoing deployment of stronger classical PKI • Active transition to RSA-4096/3072 & SHA-384 • Not Quantum Resistant
Why Increase Classical PKI?	• Strengthens against HNDL attacks • Bridges gaps until PQC is widely available • Dress rehearsal for PQC migration
Can I Skip Straight to PQC?	• No – DoW Mandate • Final legacy RSA-2048 certificate issued end of 2027 • Must support by end of 2030

Post-Quantum PKI – CNSA 2.0

- **End of 2030:** All DoW Systems must Support PQC
- **End of 2031:** All DoW Systems must exclusively use PQC
- No "drop-in" replacement
- No unapproved methods



NSA CNSA 2.0 Approved PQC Algorithms		
Usage/Function	**Algorithm**	**Standard**
Cryptographic Hash	SHA-384 or SHA-512	FIPS 180-4
Public Key Establishment	ML-KEM-1024	FIPS 203
Digital Signature	ML-DSA-87	FIPS 204
Software/Firmware Signing	LMS or XMSS	NIST SP 800-208

National Security Agency, Frequently Asked Questions, *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*, Dec 2024

CNSA 2.0 – DAF Operational Impact

- **Infrastructure Overhaul**
  - New Certificate Authorities (CAs), Sub-CAs, HSMs, Servers
- **The Interoperability Period**
  - Overlapping support for Traditional and PQC PKI
- **Cryptographic Agility**
  - Upgradability without replacement
- **Risk: Uncertain Future**
  - Uncertain upgrade paths, supply bottlenecks, and shifting timelines

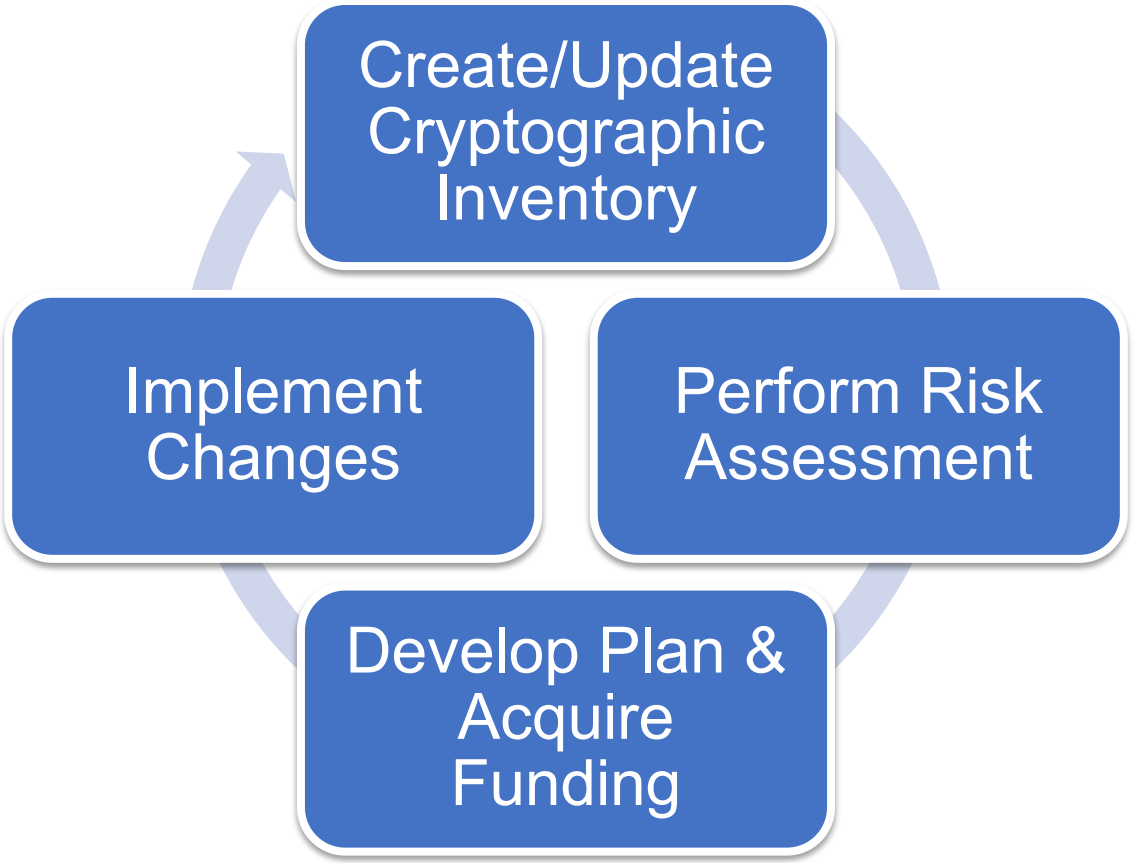
CNSA 2.0 – PKI SPO Efforts

- DAF Internal PKI Upgrade
- DoW Coordination
  - Common Access Cards and NEATS
  - SIPR Tokens
  - NPE Portal Issuance
  - Purebred and Mobility
- Communication



PQC Migration Plan

Start by selecting a PQC Migration Lead. They lead these recurring actions to meet PQC transition mandates



The Cryptographic Inventory Mandate

The Mandate

- Per OMB M-23-02, a comprehensive cryptographic inventory is the mandatory first step for both Algorithm Evolution and PQC migration

Scope

- All DoW and NSS systems
- Establish enterprise-wide inventories
- Not just PKI certificates
- No Baseline. No Funding. No Upgrade.

Visibility and Agility

- You cannot fix the unknown
- Continuous effort

Executing The Inventory - Discovery

A comprehensive, continuously maintained cryptographic inventory requires automated and manual discovery across all architectural domains:

- **Leverage Existing Tools**
- **Automated Cryptography Discovery and Inventory (ACDI)**
- **Hardware and Infrastructure**
- **Software and Applications**
- **Communication Protocols**

Executing The Inventory - Outputs

Cryptographic inventories translate data into deliverables:

- **Risk Matrix**
  - Active Compliance
  - Cryptographic Agility
- **Vendor Reliance**
- **End-of-Life (EOL) Strategy**
- **POM Request Justification**

Call to Action – DAF Leadership



- Relay requirements and accelerated timelines
- Identify channels for tracking and reporting compliance
- Assess risk and prioritize systems for transition
- Identify strategic communication channels

Call to Action – System Owners



- Perform system assessments and cryptographic inventory
- Create plan to comply with requirements within DoW timeline
- Identify unfunded requirements and develop POM
- Beware PQC “Snake Oil”: Implement only DoD-approved PQC Solutions

U.S. AIR FORCE

Call to Action – Vendors



- Review NSA and DoW timelines
- Verify support for CNSA 1.0 and 2.0 Algorithms
- Provide timelines for support to customers
- Provide compatibility attestation to NSA

We Are Here To Help

Contact US

DAF PKI SPO Website (CAC)
https://intelshare.intelink.gov/usaf-pki

DAF EITaaS ServiceNow
https://eitaas.servicecenter.af.mil/esc

Visit us at booth 168!