Super Intelligence: Post-Quantum Cryptography and Vulnerability Management

Kevin Stine
Director, Information Technology Laboratory

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

October 27, 2026

Five Decades of Digital Trust

Public cryptographic standards, built with the community, secure how we live and work



1977

DES (FIPS 46)

First public encryption standard; secured ATM networks & federal data

1995

FIPS 140 & CMVP

Validation program launched jointly with Canada

2001

AES (FIPS 197)

Chosen through an open, international competition

2015

SHA-3 (FIPS 202)

New hash family from a public competition

2019

FIPS 140-3

Module requirements aligned with ISO/IEC 19790

2024

First PQC standards

FIPS 203, 204, and 205 for the quantum era

Today, cryptography protects...

- **Personal information**
- **Commerce & payments**
- **Government systems**
- **Critical infrastructure**

NIST INFORMATION TECHNOLOGY LABORATORY

Rapidly Evolving Cryptographic and Security Landscape

Post-Quantum Cryptography

Opportunity	Standards are in place: ML-KEM, ML-DSA, SLH-DSA
Challenge	Every system must migrate, with federal deadlines in 2030 and 2031
Validation	A wave of PQC modules, with new test methods and guidance

Super Intelligence (SI)

Opportunity	Develop stronger standards
Challenge	Potential for new weaknesses or flaws, driving need for crypto-agility
Validation	New test methods, and trust in SI-assisted evidence

A National Priority

Executive Order 14412

Securing the Nation Against Advanced Cryptographic Attacks | Signed June 22, 2026 (building on NSM-10)

Year: 2030
Key establishment

Year: 2031
Digital signatures

Deadlines for federal High Value Assets and high-impact systems

What the order requires

- Accelerates PQC migration for the government's highest-risk systems
- OMB and the Office of the National Cyber Director lead the national migration across agencies, critical infrastructure, and industry
- Directs the FAR Council to update acquisition rules so contractors comply with NIST's PQC standards

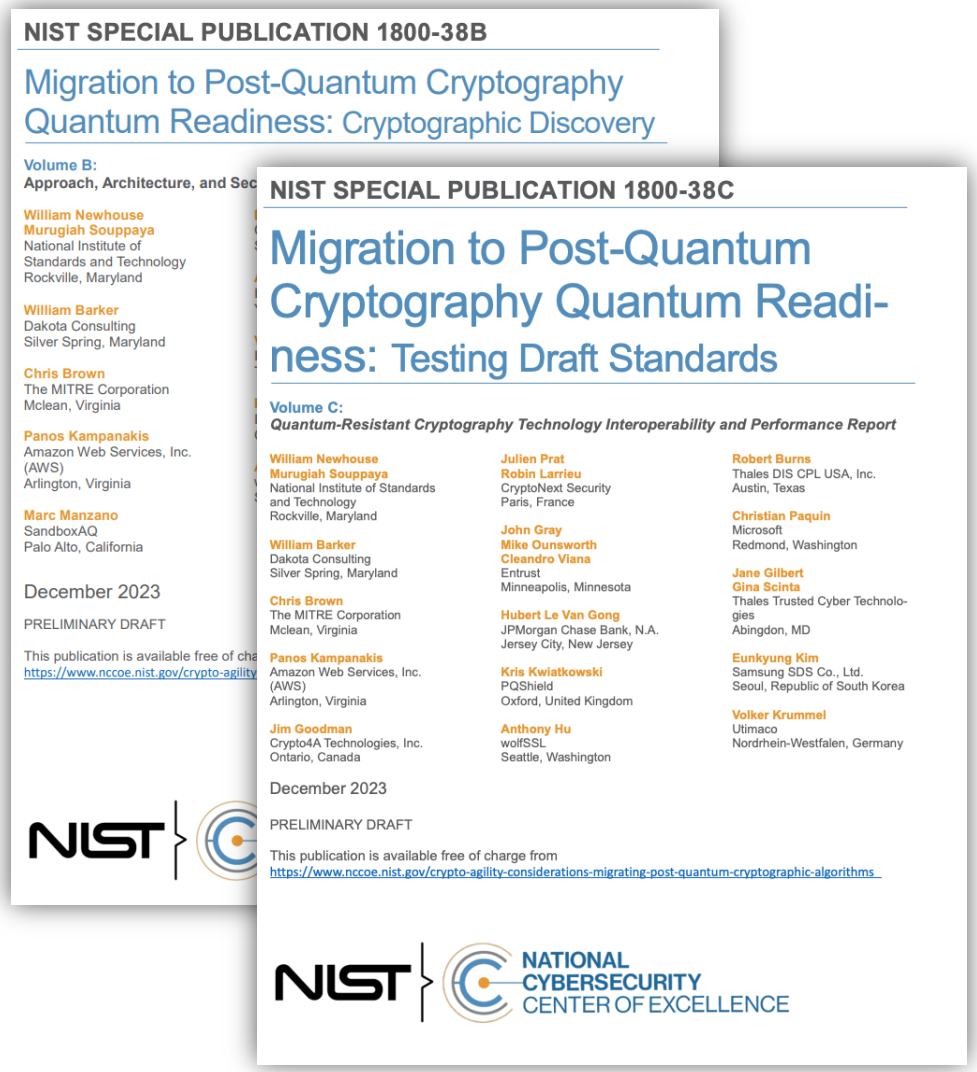
NIST's central role

- Ongoing PQC implementation guidance for agencies, with NSA and CISA
- Launch pilot migration on NIST systems by 2027
- Accelerated validation of PQC modules through the Cryptographic Module Validation Program (CMVP)
- Support to the State Department to encourage foreign governments to adopt NIST-standardized PQC

NIST INFORMATION TECHNOLOGY LABORATORY

Accelerating Adoption

- At NIST's National Cybersecurity Center of Excellence (NCCoE), we are tackling challenges with ***adoption, implementation, and deployment*** of PQC in applications and protocols
- Engage with ***over 60*** industry and government partners to ***increase awareness*** and ***demonstrate practices*** that help organizations migrate to post-quantum algorithms
- Coordinate with ***standards developing organizations*** and ***government/industry*** to develop guidance to accelerate the migration
- Support ***U.S. Government PQC initiatives***
  - NSM-10
  - Quantum Computing Cybersecurity Preparedness Act
  - NSA CNSA 2.0



NIST INFORMATION TECHNOLOGY LABORATORY

Global Acceptance

Governments and standards bodies worldwide have adopted or endorsed the NIST PQC algorithms

ML-KEM (FIPS 203) **ML-DSA** (FIPS 204) **SLH-DSA** (FIPS 205)

GOVERNMENTS

United States
CNSA 2.0 requires ML-KEM & ML-DSA for national security systems

Europe
German, French & EU migration plans build on the NIST algorithms

UK, Canada & Australia
National migration roadmaps centered on the NIST algorithms

Asia-Pacific & Gulf
Japan, Korea, Singapore & Saudi Arabia profiling NIST algorithms

STANDARDS BODIES

IETF
ML-KEM key exchange in TLS; NIST signatures in X.509 & CMS

ISO/IEC
Incorporating the NIST algorithms into international standards

ETSI, 3GPP & GSMA
Quantum-safe profiles for telecom & 5G networks

Platform & PKI bodies
TCG, GlobalPlatform & CA/B Forum: Secure elements & certificates

NIST algorithms are the common thread across nations and SDOs – the basis for global interoperability.

The Power of SI Tools

SI tools strengthen researchers' ability to evaluate the security of cryptographic algorithms, but adversaries could also use SI tools to discover unknown weaknesses, particularly in algorithms that have not been sufficiently scrutinized.

INTEGRATING SI TOOLS INTO NIST'S PROCESSES

1. **Research & analysis**
   Using SI tools to support cryptanalysis and the security evaluation of candidate algorithms
2. **Test tool development**
   Supporting development of validation test tools for cryptographic algorithms
3. **Standards validation**
   Checking the documentary standards that NIST develops for consistency, errors, and security

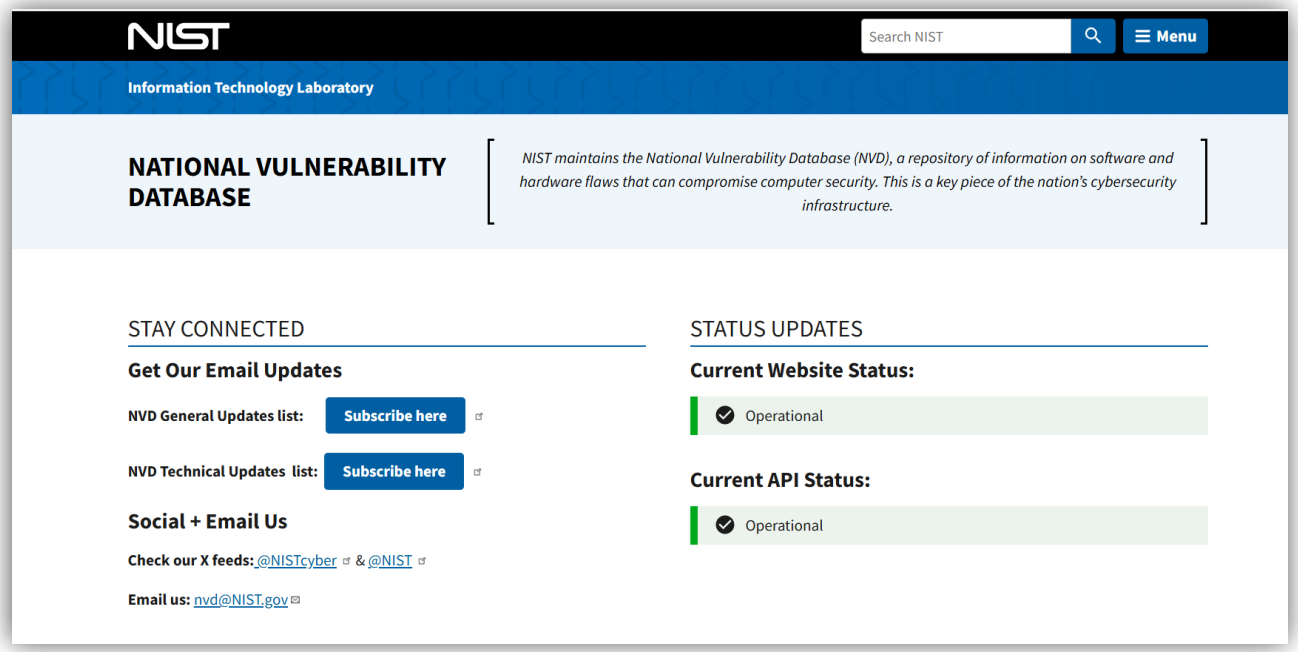
Partnerships

NIST is working to establish partnerships with tool developers and researchers to advance the use of SI tools for cryptography.

NIST INFORMATION TECHNOLOGY LABORATORY

On Sept. 29, 2026, the Executive Order on Inaugurating the Era of Super Intelligence directed executive agencies to update its use of "artificial intelligence (AI)" to "super intelligence (SI)."

National Vulnerability Database (NVD)

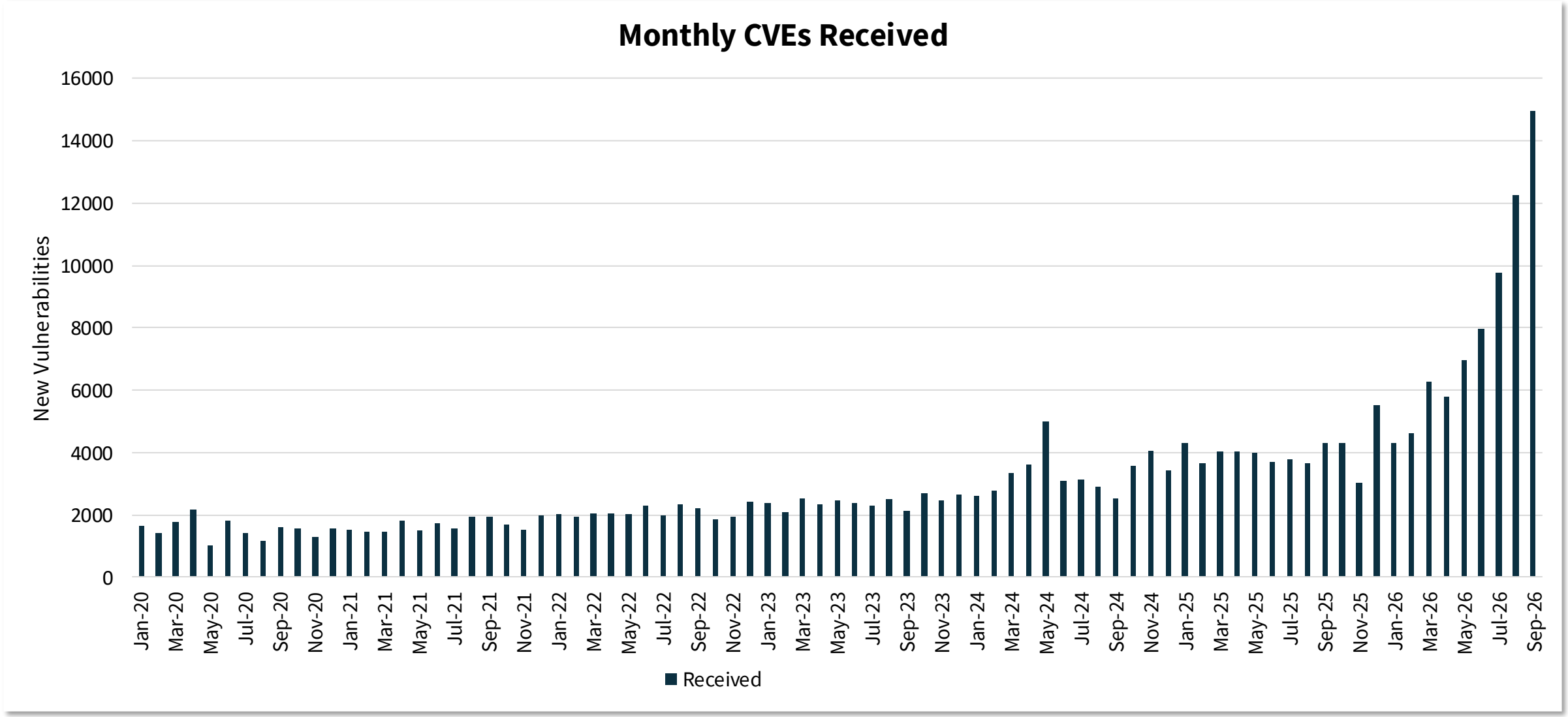


The NVD is a repository of information on software and hardware flaws that can compromise computer security.

This is a key piece of the nation's cybersecurity infrastructure.

NIST INFORMATION TECHNOLOGY LABORATORY

The Growing NVD Landscape



How We're Adapting

1

CPE Specification Update

- Address identification and naming of hardware
- Enable federation

2

Request for Information (RFI)

- Improve scalability, automation, interoperability, transparency, utility

(*Released on 8/12/2026)*
(Comments closed 10/13/2026)

3

SI Agent

- Encourage automation
- Testing new tool internally

(*Potential future public release)*

We are responding with innovative plans and updates to take us into the future.

Questions?



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

NIST.gov/itl

@NIST
@NISTcyber