State of the PQC Migration

Moses Liskov

Principal Cryptographer and Cybersecurity Engineer, MITRE

October 27, 2025

Post Quantum Cryptography Coalition

MITRE

Policies and Mandates

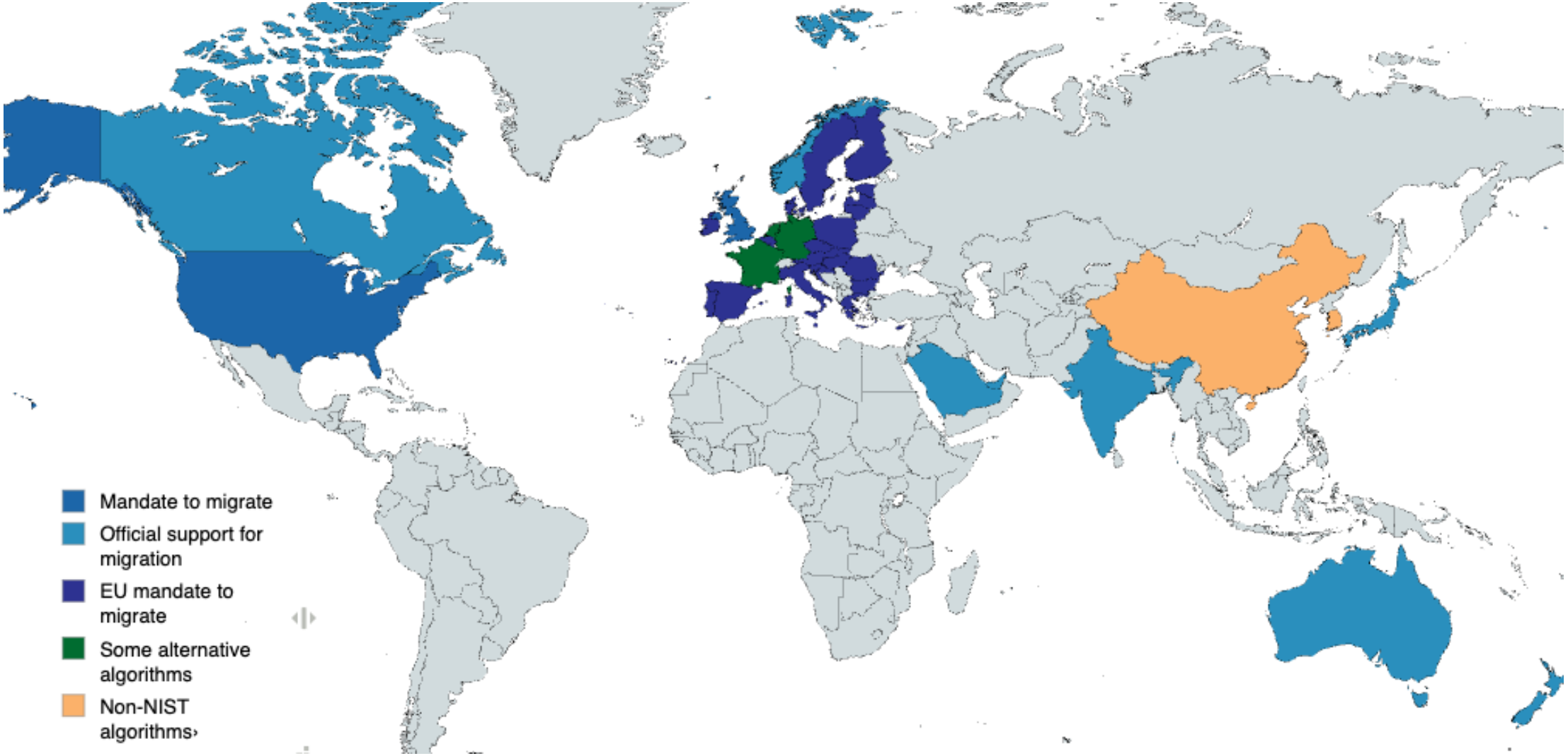
White House / Presidential Orders
NSM-8 – post-quantum in NSS
NSM-10 – migration all of gov't by 2035
M-23-02 – requires inventories & budget estimates
EO 14144 / EO 14306 – other quantum-related steps

NSA policies
CNSA 2.0 – algorithms & plans for NSS

NIST official status
NIST SP 800-131r3 – "acceptable" status for PQC
NIST IR 8547 (ipd) – deprecation plan for 2030/2035

Quantum Computer Cybersecurity Preparedness Act (Public Law 117-260)

International requirements



PQC Standardization and Adoption

Standard	Overall Range	Pure PQ encrypt	Hybrid PQ encrypt	Pure PQ sig	Hybrid PQ sig
SSH	3 to 8	3	8	3	3
TLS 1.2[1]	0 to 0	0	0	0	0
TLS 1.3[2]	3 to 9	7	9	7	3
X.509[3]	4 to 7	7	4	7	6
S/MIME	3 to 7	7	3	7	3
OpenPGP	2 to 4	2	4	4	4
IKE / IPSec	3 to 8	8	8	4	3
MLS	2 to 4	4	4	4	2
TPM	2 to 4	4	2	4	2
DNSSec	1 to 1	-	-	1	1

1: DTLS 1.2, FIDO inherit from TLS 1.2

2: DTLS 1.3, MACSEC, FIDO/FIDO2 inherit from TLS 1.3

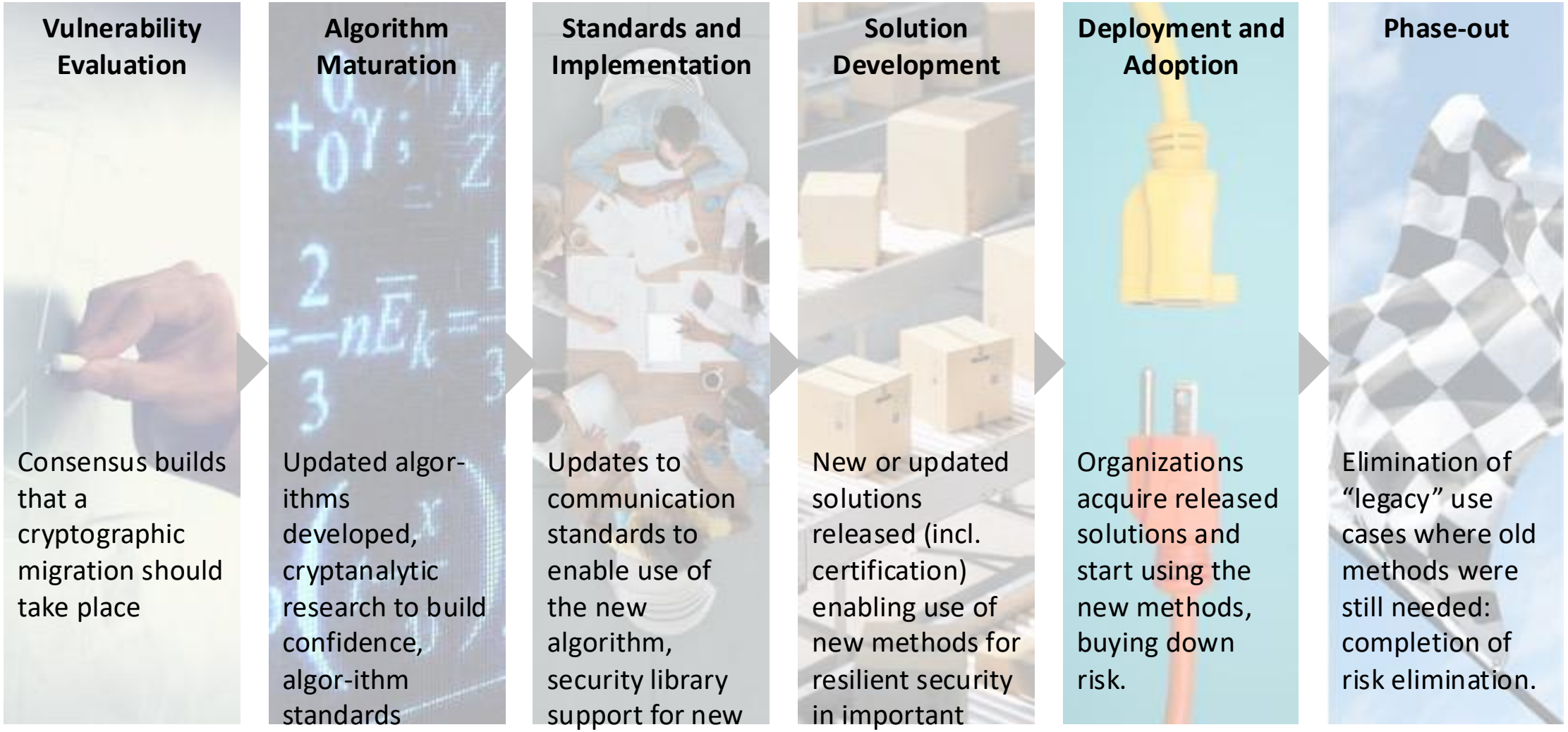
3: UEFI inherits from X.509

Key

0	Consensus Against Inclusion
1	Blocked / Stalled
2	In Progress / Chartered
3	Active Proposals / Drafts
4	Progress to Finalization
5	Finalized / Approved
6	Integration Progress
7	Integrated in Libraries
8	Some Adoption
9	Broad Adoption
-	Unknown / NA

MITRE Post Quantum Cryptography Coalition

Phases of a Cryptographic Migration



Vulnerability Evaluation

Consensus builds that a cryptographic migration should take place

Algorithm Maturation

Updated algor-ithms developed, cryptanalytic research to build confidence, algor-ithm standards finalized.

Standards and Implementation

Updates to communication standards to enable use of the new algorithm, security library support for new methods.

Solution Development

New or updated solutions released (incl. certification) enabling use of new methods for resilient security in important products.

Deployment and Adoption

Organizations acquire released solutions and start using the new methods, buying down risk.

Phase-out

Elimination of “legacy” use cases where old methods were still needed: completion of risk elimination.

MITRE Post Quantum Cryptography Coalition

Challenge: Normalizing information between vendors

Technical Milestone	Description
Blocked	Critical standards or implementations are not sufficiently mature
Enabled	Prerequisites are known to be met, enabling further progress
Components	Components of a full or partial solution have been announced
Partial Solution	Solution with partial PQC enablement has been announced
Full Solution	Solution with full PQC enablement has been announced

Commitment Milestone	Description
No Information	No specific discussion of the migration known / public
General Interest	Source shows awareness / tracking of the migration
Intent	Source expresses intent to achieve PQC enablement, without details
Roadmap	Source reveals details of steps towards achieving PQC enablement
Timeline	Source makes specific time commitment to achieving full PQC enablement
Completion	Source has achieved full solution; no further commitments necessary

Pre-release capability heatmap

Capability	One		Segment		Many/All	
Web Browser	4	5	4	3	4	3
Web Server	4	5	4	3	4	3
VPN / network encryption	4	3	4	3	2	2
Platform Assurance (Firmware Signing / TPM)	3	1	2	1	1	1
Code Signing / Patch Management	2	5	2	1	1	1
PKI / CA Management	3	5	3	1	3	1
Volume Encryption	?	1	?	1	?	1
Database Data Protection	?	1	?	1	?	1
Cloud Service Connectivity	4	4	4	3	4	3
Zero Trust	?	1	?	1	?	1

KEY

Technical milestones

1	Blocked
2	Enabled
3	Components
4	Partial Solution
5	Full Solution

Commitment milestones

1	No Information
2	General Intent
3	Intent
4	Roadmap
5	Timeline
6	Completion

MITRE Post Quantum Cryptography Coalition