



Post-Quantum Cryptography

What it is, why it matters to New Mexico, and what to do about it

Raja Sambandam, CISSP, CRISC, CISA
State Chief Information Security Officer

Our digital locks need an upgrade



TODAY'S LOCK

Protects state data with math ordinary computers can't solve



TOMORROW'S QUANTUM KEY

A large quantum computer could unlock it

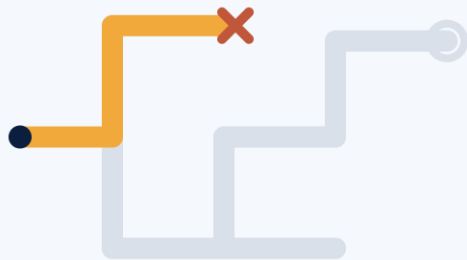
The answer: upgrade the lock before that key exists — to protect New Mexicans' data and our economy.

The Ultimate Super-Computer



NORMAL COMPUTER

Rides down one path at a time



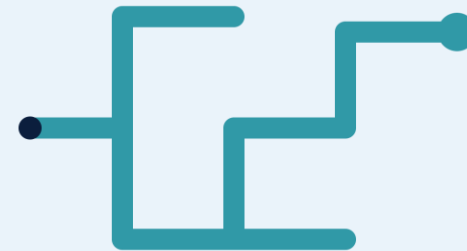
Years

to break today's standard encryption



QUANTUM COMPUTER

Explores many paths at once



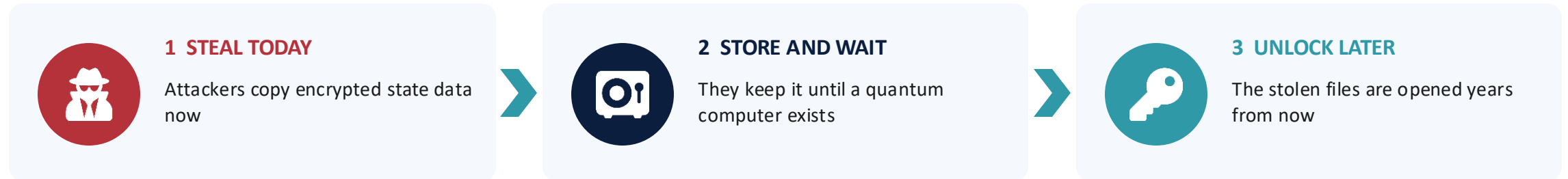
Hours

for a future, large machine — none exists yet

Estimates vary with assumptions. "Hours" is a published research estimate for a machine with about 20 million qubits.



Why Our Current Codes Will Fail



HOW LONG NEW MEXICO RECORDS MUST STAY SECRET (STATE RULES)



Data stolen today has to stay secret long after a quantum computer could exist.



Post-Quantum Cryptography (PQC)

New math that resists both quantum and ordinary computers — standards finalized by National Institute of Standards and Technology in August 2024.



FIPS 203 · ML-KEM

Safely shares the keys that lock data as it travels

FIPS 204 · ML-DSA

Digital signatures that prove who sent something

FIPS 205 · SLH-DSA

A backup signature method built on different math

Typically, Hardware, Software, System Configurations and Testing — Outdated systems that can't be upgraded would require replacing.



The NIST Standards and Federal Deadlines



OFFICIAL DATES

- AUG 2024** NIST finalizes the new standards (FIPS 203, 204, 205)
- JAN 2027** New national-security system purchases must be quantum-safe (NSA)
- DEC 31, 2030** Federal high-value systems and federal contractors must switch (EO 14412)
- DEC 31, 2031** Federal digital signatures must switch (EO 14412)
- 2035** Goal: all federal systems moved and the old locks retired

Today is October 8, 2026. These deadlines bind federal agencies and contractors — New Mexico inherits them through vendors and federal data.



Why Our State Must Act



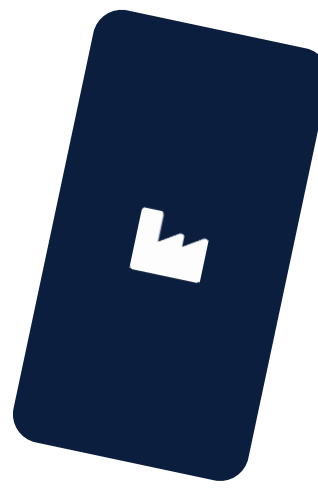
NIST retires the old locks

deprecated 2030, retired 2035



Federal data rules follow

FBI CJIS and IRS Pub. 1075 require the latest NIST-validated encryption



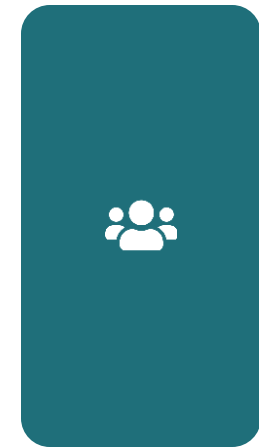
Vendors must switch

federal contractors by end of 2030 (EO 14412)



NM state and local systems

share federal data and buy from those vendors



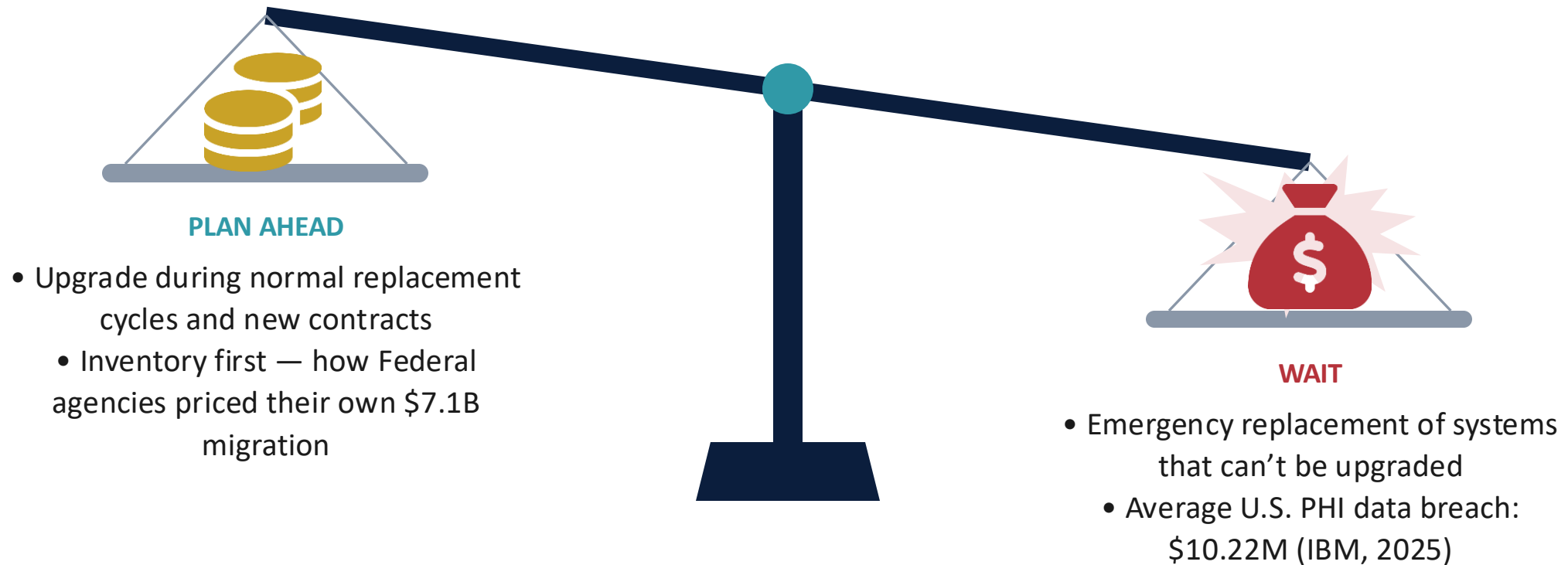
New Mexicans' data

tax, health, court and police records

It already happened: on Sept. 21, 2026, NIST retired the older FIPS 140-2 encryption standard — and state agencies handling criminal-justice data must now plan around it. Quantum-safe encryption will follow the same path. Without state mandate we may quickly end up with a patchwork of systems that may not be PQC safe.



Smart Spending vs. Emergency Crises



Upgrading on schedule costs less than replacing systems in a rush — **and the inventory tells us which is which.**



Finding the Vulnerable Locks

Sample scan of a state system

web.key_exchange	= ECDHE P-256	⚠ quantum-vulnerable
vpn.handshake	= RSA-2048	⚠ quantum-vulnerable
email.signature	= RSA-2048	⚠ quantum-vulnerable
db.storage	= AES-256	✓ safe (symmetric keys)
vendor.app.login	= unknown	? ask the vendor

MOST SENSITIVE DATA FIRST

- Personal information (PII)
- Health records (PHI)
- Payment card data (PCI)
- Student records
- Water and utility control systems

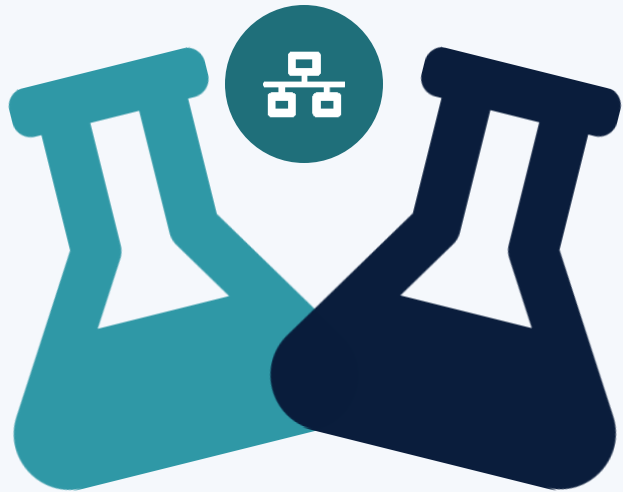
STEP 2 OF THE CISA, NSA AND NIST PLAYBOOK



We can't fix what we can't find. The inventory is the cheapest step — and it produces New Mexico's real cost number.



Collaborating with Sandia & Los Alamos



SANDIA

LOS ALAMOS

Both help DARPA test whether quantum computers really work

2

national labs in New Mexico — Sandia runs DOE's longest-running quantum computing program

Up to \$120M

DARPA–New Mexico partnership: up to \$60M each over four years, based on results

0 → 5

quantum companies set up in New Mexico in under two years

1 of 2

New Mexico is part of one of the 2 federal quantum Tech Hubs (31 hubs nationwide)

The opportunity: world-class quantum expertise is already in New Mexico — OCS proposes to tap it for the state's transition.



Partnering with Higher Education



UNM Quantum New Mexico Institute

CNM co-led the federal Tech Hub application

QUANTUM JOBS — COLORADO, NEW MEXICO AND WYOMING COMBINED (HUB FIGURES)

Working today



Goal, next 10 years



Over half

of quantum jobs don't need a graduate degree, community colleges and universities can train for them (independent analysis)

The payoff: New Mexicans trained for these jobs keep high-paying tech careers — and the transition work — in our state.



Updating Our State Purchasing Rules

STATE OF NEW MEXICO

IT Purchase Contract

**NIST PQC
COMPLIANT**

THE MARKET IS ALREADY MOVING



SEPT 2026

Only newer FIPS 140-3 validated encryption accepted for new federal purchases



2029

Google and Cloudflare: fully post-quantum



END 2030

Federal contractors must use the new standards (EO 14412)



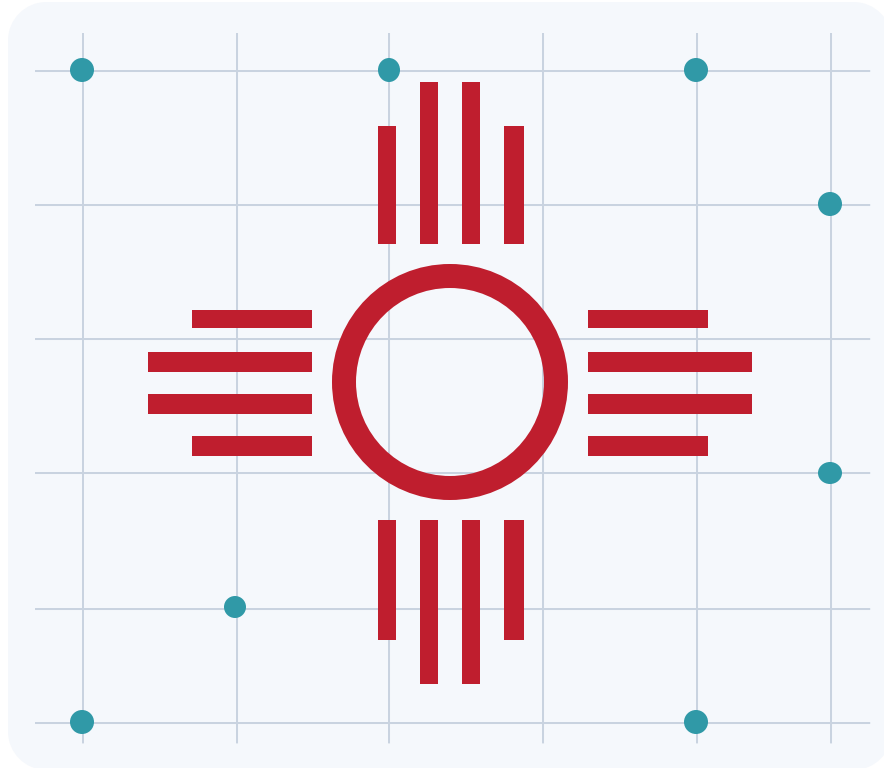
2033

Microsoft: fully post-quantum

The ask: every new state IT contract requires NIST quantum-safe encryption, checked through third-party risk management.



Securing New Mexico's Legacy



OCS leads

One lead office runs the inventory and the statewide transition



Labs advise

Sandia and Los Alamos expertise guides the work



Universities train

UNM, CNM and partners build the workforce

HOW YOU CAN HELP

- Require the inventory, on a deadline
- Fund Phase 1: the inventory
- Require PQC-compliant state contracts

We protect our citizens, protect our economy — and lead the nation.



The Cost of Getting New Mexico Compliant



\$1M

*First-round request, FY27–FY28:
inventory of priority state systems.*

- Initial request would be 1M for completing the inventory of Hardware/Software of weaker encryption keys
- Once the inventory is complete, we will have a better understanding of the total cost including replacements and upgrades.



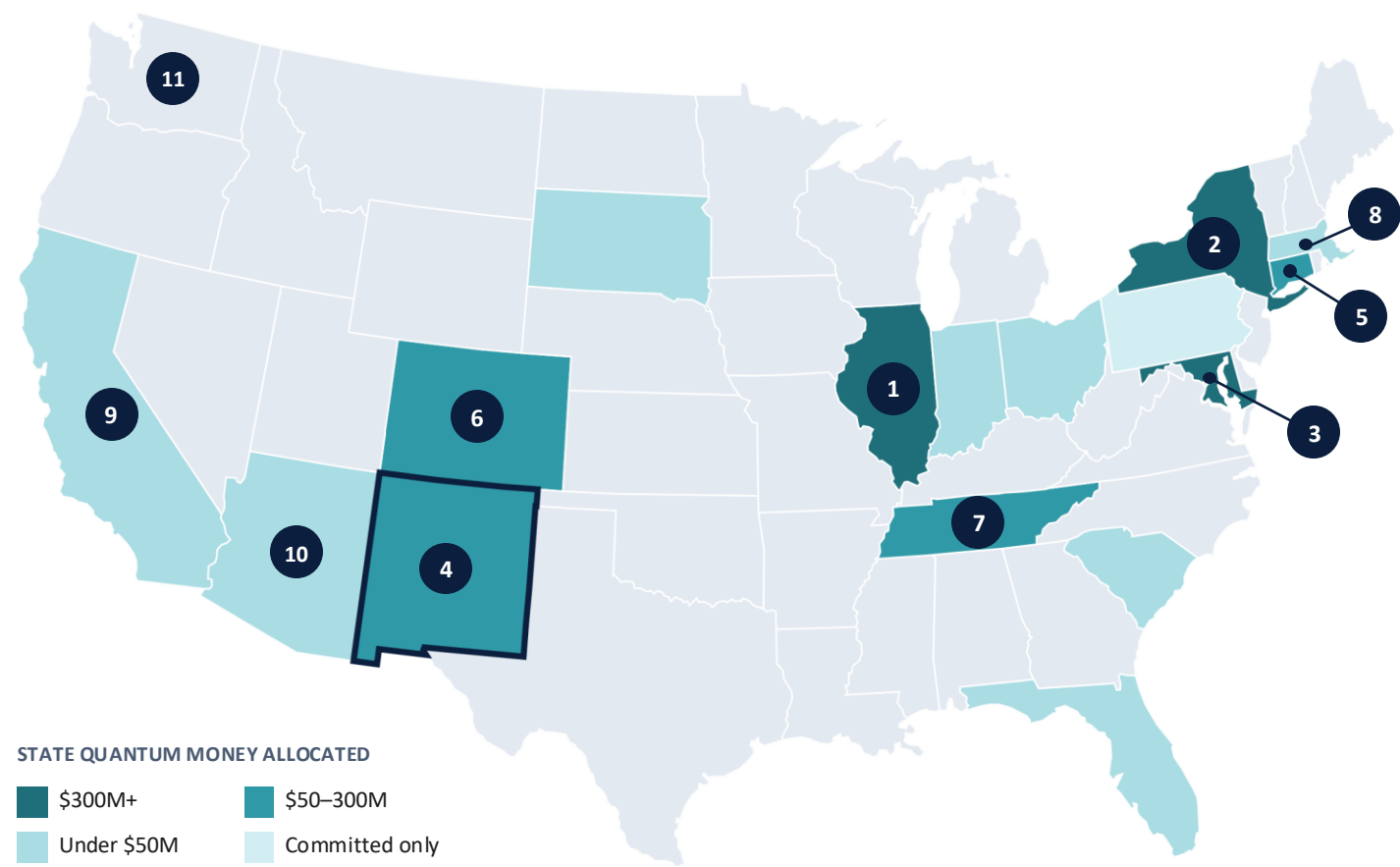
WHY THIS IS A GOOD BET

The state rarely writes its own encryption — it's embedded in the products it buys. The two highest-value early moves (inventory + procurement requirements) cost little; the expensive part is upgrading legacy systems that can't be made crypto-agile — which is exactly why funding the inventory first controls the total bill.



Who’s doing what, state by state

Per an independent tracker, New Mexico ranks 4th in state quantum money allocated — 2nd counting committed funds.



LINE 1: PUBLIC MONEY LINE 2: PRIVATE COMPANIES

- 1 Illinois** \$726M state · leads The Bloch Tech Hub
IBM, PsiQuantum, Infleqtion at the state quantum park
- 2 New York** \$367M state
IBM Quantum — \$1B federal award for a U.S. quantum foundry
- 3 Maryland** \$302M state · \$1B public-private goal
IonQ headquarters · Microsoft quantum research center · IQM
- 4 New Mexico** \$167M state + \$255M committed · Tech Hub partner
Quantinuum, QuEra, Qunnect, Maybell Quantum, Mesa Quantum
- 5 Connecticut** \$86M state · NSF Quantum Engine (Yale, UConn)
Startups backed by a \$50M state AI/quantum fund
- 6 Colorado** \$78M state · leads Elevate Quantum
Quantinuum, Infleqtion, Maybell — largest cluster (per hub)
- 7 Tennessee** \$65M state · EPB quantum network (Chattanooga)
IonQ
- 8 Massachusetts** \$39M state + \$40M committed
QuEra (Boston)
- 9 California** \$14M state
Google Quantum AI, Rigetti, PsiQuantum, AWS
- 10 Arizona** \$9M state · first state post-quantum bill (HB 2809)
- 11 Washington** No state figure in tracker
Microsoft · IonQ quantum computer factory

State dollars: The Quantum Insider state tracker, Q3 2026.

Sources & key numbers

- **Market & timeline** McKinsey Quantum Technology Monitor 2026 \$1.3–\$2.7T by 2035; ~\$12.6B invested in 2025; IBM fault-tolerant target ~2029.
- **Encryption risk** NIST post-quantum standards (FIPS 203/204/205, 2024) and NIST IR 8547 (2030/2035). IBM Cost of a Data Breach 2025 (U.S. average \$10.22M).
- **New Mexico** U.S. EDA Tech Hubs / Elevate Quantum; NM Economic Development Dept. and UNM (Quantum NM Institute); \$25M venture studio (2025); FLC award (2026). State dollars: [The Quantum Insider state tracker](#).

OTHER STATES ON THE MAP (SLIDE 15)

Dollar figures for every state: [The Quantum Insider state tracker, Q3 2026](#)

Illinois

[Governor of Illinois](#) · [EDA: The Bloch Tech Hub](#)

New York

[NIST/Commerce: IBM \\$1B CHIPS award](#)

Maryland

[Governor of Maryland](#) · [The Quantum Insider](#) · [Quantum Computing Report](#)

Connecticut

[Yale News: \\$121M state pledge](#) · [CT Mirror: NSF Engine](#)

Colorado

[Colorado OEDIT](#) · [Elevate Quantum](#) · [Quantinuum](#)

Tennessee

[SCSP: Quantum States \(EPB, IonQ\)](#)

Massachusetts

[Entangled Future: U.S. quantum landscape](#)

California

[Entangled Future](#) · [Rigetti](#) · [Quantum Zeitgeist \(AWS\)](#)

Arizona

[Arizona Legislature: HB 2809](#) · [JLBC fiscal note](#)

Washington

[CT Mirror: IonQ factory](#) · Microsoft HQ, Redmond (public record)



Thank you



Questions