

The Future of Encryption:

Preparing Government for the
2030 Post-Quantum Shift

Craig Costello



YOUR DEADLINE ALREADY EXISTS

Q-day remains uncertain

2030

THE FIRST MILESTONE IS THIS YEAR

2026

Refined plan

2028

Transition underway

2030

Transition complete

ASD recommended milestones, by year-end

Q-DAY IS THE WRONG CLOCK

HARVEST NOW

The copy can exist today

Data lifetime + migration time

DECRYPT LATER

The harm can arrive years later

WHY Q-DAY COULD COME SOONER

Better Shor circuits

Less error-correction overhead

≈ 20×

fewer physical qubits

ECDLP-256 / secp256k1 estimate

March 2026 estimates. Q-day remains uncertain.

**WHAT ACTUALLY
BREAKS?**

TRUST

Identity

Connections

Software



THE CRYPTO IS READY

Deployment is
the hard part



CRYPTO AGILITY

AI-assisted cryptanalysis

60 HOURS

To find and verify an improved HAWK attack

Research candidate, not a deployed standard

Anthropic, July 2026

Replace algorithms. Keep services running.

PQC is the test case



YOUR VENDORS SET THE PACE

Your agency owns the risk



YOUR NEXT CONTRACT NEEDS A PQC UPGRADE PATH

When can we test it?

Who pays for the upgrade?

FIND IT.

PRIORITISE IT.

START MOVING.

A named owner. A funded plan.