QUANTUM CORE INSTITUTE

QCI-QS1-S3

State and Local Government Supplement

Quantum Readiness Guidance for State Agencies, County Governments, and Municipal Authorities

Document ID	QCI-QS1-S3
Version	1.2
Status	Public — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Applies to	State agencies, county governments, municipal authorities, and their technology service providers handling citizen data and critical government systems
Effective date	September 23, 2026
Review cycle	Annual, or upon material CISA, NIST, OMB, or state cybersecurity office developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for the specific regulatory, procurement, and operational context of state and local government. It maps quantum readiness requirements to federal policy, CISA guidance, NIST post-quantum standards, and the legacy system and procurement cycle realities that define cryptographic exposure for most government entities in this sector.

Foreword

State and local government is the most underserved sector in quantum readiness. Federal agencies have NIST guidance, OMB memoranda, an executive order with dates, and dedicated cybersecurity budgets. Large enterprises have security teams and vendor relationships that put quantum risk on the agenda. State and local government — where the majority of citizen-facing public services operate, where decades of property records and vital statistics are stored, and where legacy systems have procurement cycle lifespans measured in decades — has almost nothing specifically tailored to its situation.

That gap is the opportunity and the problem simultaneously. State CISOs and county IT directors who want to address quantum risk have to translate federal guidance designed for cabinet agencies into a context that looks nothing like a cabinet agency. They have to justify budget requests to officials who may not have a technical background. They have to engage legacy platform vendors whose upgrade cycles are governed by legislative appropriations, not product roadmaps. And they have to do all of this with staffing levels that most private sector security teams would consider inadequate for basic operations.

This supplement translates QCI-QS1 for that context. It does not simplify the threat. Quantum computing will break the cryptographic infrastructure protecting citizen data, election systems, property records, and public safety communications on a timeline that is relevant to systems being procured and contracts being signed today. What this supplement does is give state and local government entities the specific framework, regulatory mapping, and practical guidance to begin addressing that threat within the constraints they actually face.

The governments that act now will not need to scramble when federal deadlines reach them through grant conditions and interoperation, when state cybersecurity laws are updated to include quantum readiness, or when a peer jurisdiction suffers the first quantum-enabled breach of a government system. They will be the ones setting the standard.

What changed in version 1.2

Version 1.2 aligns this supplement to QCI-QS1 version 2.3 and updates the federal policy context. Executive Order 14412 (June 22, 2026) and OMB M-26-15 (June 24, 2026) replace the earlier memorandum as the federal benchmark and set dated deadlines that reach state systems through grants and interoperation; section 2.1 is rewritten and section 2.4 turns the mapping into the obligations register QCI-2.2-01 requires. Three scoring changes matter: the Defensible readiness band now begins at 81; gate G70 is no longer satisfied by a documented exception, so an entity cannot score above 70 until every critical vendor and service provider has attested (section 4.5); and gate G60 is fixed at 95 percent validated coverage of both critical systems and critical data flows.

1. Scope and applicability

This supplement applies to:

- State executive branch agencies and departments, including those handling health and human services, revenue and taxation, motor vehicles, public safety, and elections
- County and parish governments, including those operating courts, health departments, property assessment systems, and public safety communications
- Municipal governments, utilities, and authorities operating citizen-facing services, payment systems, and public safety infrastructure

- State and regional public safety communications networks, including those using encrypted radio and data systems
- Technology service providers and systems integrators under contract to provide IT services to government entities in scope

This supplement is proportional by government tier. A state agency with a dedicated IT security team is expected to implement QCI-QS1 at greater depth than a rural county with a single IT generalist. Where requirements differ by tier, this is explicitly noted. Proportionality does not change the gates: the coverage threshold and the supplier attestation requirement apply to whatever assessment boundary the entity declares (QCI-1.1-01), and a small boundary is easier to cover than a large one.

Why government is different from private sector

Three characteristics define quantum readiness in government that do not apply in the same way to private sector organizations. First, procurement cycles: a state agency that needs to upgrade a cryptographic system may require a legislative appropriation, a competitive RFP process, and a multi-year implementation — a timeline measured in years, not months. Second, legacy system tenure: government systems routinely operate for 15 to 25 years, meaning systems procured today will still be running when quantum computers capable of breaking current encryption are available. Third, public accountability: a breach of citizen data held by a government entity carries political consequences that private sector data breaches typically do not. These three characteristics make early action more valuable in government than in almost any other sector.

Note on the AI-cryptographic provisions

QCI-QS1 carries conditional AI-cryptographic provisions. Where AI systems fall within the assessment scope — for a government entity, most often a benefits eligibility, document processing, or citizen-service tool operated by a vendor — the organization also keeps linked AI artifact records with separate confidentiality and verification horizons (QCI-5.2-03), exercises the D7-AI incident scenarios (QCI-4.4-03), includes AI suppliers' posture in Pillar 5 (QCI-6.4-01), and issues Annex C section G, questions G1 to G5, to suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts. These provisions have no effect where AI systems are not in scope; a non-AI system records AI applicability as none. They govern cryptographic risk arising from AI systems. They do not govern AI risk generally.

2. Regulatory and policy context

2.1 Federal policy applicable to state and local government

State and local governments are not directly subject to the federal cybersecurity mandates that apply to federal agencies. However, federal policy creates the benchmark that state cybersecurity offices, federal grant programs, and eventually state legislation reference, and since June 2026 that benchmark carries dates. The following federal actions are directly relevant. QCI-QS1 Annex E records them as S1 to S3, S12 and S13; applicability to any particular state system is a determination the entity makes under QCI-2.2-01, with counsel.

Federal action	Key requirement or guidance	State and local relevance
NIST Post-Quantum Cryptography Standards (FIPS 203, 204, 205)	Define the approved post-quantum algorithms. Federal agencies are required to migrate.	State systems receiving federal funding or interoperating with federal systems will be expected to align. Sets the algorithm standard that approved cryptographic profiles under QCI-4.5-01 should target.
Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (June 22, 2026)	Directs federal agencies to complete post-quantum key-establishment transition for high-value and high-impact systems by December 31, 2030 and authentication transition by December 31, 2031, and directs rulemaking toward contractor requirements.	The dates propagate to state systems through federal interoperation (tax, health and human services, public safety data exchange) and through grant and contract conditions as rulemaking completes. Record in the obligations register as federal policy with applicability by contract or interoperation.
OMB M-26-15, Execution of the Migration to Post-Quantum Cryptography (June 24, 2026)	Federal civilian agency implementation policy: migration plans, prioritization, supplier engagement, and a phased approach distinguishing priority systems from the remaining estate. Functionally supersedes M-23-02.	The planning methodology benchmark for states with federal grant-funded IT systems. Its prioritization logic — high-value and long-lived data first — matches the compounding HNDL lens in section 3.2.
CISA Post-Quantum Cryptography Initiative	Sector-specific guidance and toolkits for critical infrastructure and government.	CISA guidance is the primary federal resource for state and local government quantum readiness. The QCI-QS1 framework maps cleanly to CISA's recommended program elements.
Executive Order 14028 on Improving the Nation's Cybersecurity (2021)	Federal agencies required to adopt zero trust and modernize security posture.	Historical context for the current program; the zero-trust and software-supply-chain requirements it introduced remain the frame that EO 14412 builds on.
State and Local Cybersecurity Grant Program (SLCGP)	DHS grants to states for cybersecurity improvements. Requires cybersecurity plans.	Quantum readiness is an eligible activity under SLCGP. A documented QCI-QS1 program supports grant applications and demonstrates alignment with federal PQC migration priorities.

2.2 State-level regulatory environment

The state regulatory environment for cybersecurity is evolving rapidly. Thirty-six states had enacted cybersecurity legislation affecting state agencies as of early 2026. The following state-level developments are directly relevant to quantum readiness:

- State cybersecurity laws: States including New York, California, Texas, Virginia, and Colorado have enacted or are developing cybersecurity requirements for state agencies that reference federal NIST frameworks. As NIST incorporates PQC standards, these state laws will implicitly require PQC compliance for covered agencies.

- State CISO authority expansion: Many states have moved their CISO from an advisory role to a governance role with authority to mandate security standards across agencies. A state CISO who adopts QCI-QS1 as the quantum readiness standard creates a mandate for all agencies under their authority.
- Election system security: The Election Assistance Commission and state election officials are beginning to address quantum risk to election infrastructure specifically. States that conduct their own election security programs should treat election systems as among the highest-priority QASI inventory targets.
- Public safety communications: States operating P25 or FirstNet-adjacent public safety communications networks should monitor DHS and FCC guidance on quantum resilience for emergency communications infrastructure, where cryptographic compromise has direct public safety consequences.

2.3 The SLCGP funding opportunity

The State and Local Cybersecurity Grant Program represents a direct funding mechanism for quantum readiness work. QCI-QS1 implementation activities — governance establishment, QASI inventory, vendor engagement, Q-Risk Score assessment — are eligible activities under the program's cybersecurity plan requirements.

States that include quantum readiness as a line item in their SLCGP cybersecurity plan are better positioned for grant approval than those that do not, because they demonstrate alignment with federal PQC migration priorities, which now carry the EO 14412 dates. The QCI-QS1 documentation artifacts — QASI, Q-Risk Score, vendor attestations, governing-body insert — directly satisfy the program's planning documentation requirements.

Using QCI-QS1 to support SLCGP applications

A state that can demonstrate a current Q-Risk Score with its assessment type stated, a documented QASI covering critical systems and flows, and an active vendor engagement program aligned with NIST PQC standards has a materially stronger SLCGP application than one that describes quantum risk in general terms. The QCI-QS1 evidence standard (QCI-4.8-01) is designed to produce exactly the documentation that grant reviewers look for when assessing program maturity.

2.4 Obligations register entries for this sector

QCI-2.2-01 requires an applicability register listing each relevant external obligation with its issuer, exact document and revision, date, authoritative URL, applicable sections, status, affected systems and suppliers, required actions and deadlines, exception authority, accountable owner, and last verification date. The federal table in section 2.1 and the state list in 2.2 are the seed. The entries below are the minimum; each entity adds its state statutes, its grant conditions, and any federal data-exchange agreements, and verifies every entry against the source. A general migration target such as 2035 never overrides an earlier applicable deadline.

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Federal PQC transition	EO 14412; OMB M-26-15	Federal policy; applies to the entity only by contract, grant condition, or federal interoperation	Systems exchanging data with federal agencies; grant-funded systems	Confirm applicability with counsel; where applicable, key establishment by December 31, 2030 and authentication by December 31, 2031
Grant conditions	DHS SLCGP; other federal grant programs	Contract	Grant-funded systems and their vendors	Include quantum readiness in the cybersecurity plan; retain QCI-QS1 artifacts as program documentation
State cybersecurity law	State statute and CISO standards, as enacted	Law and regulation	Covered agencies and their service providers	Track amendments that incorporate NIST PQC standards; record the revision
Records retention	State records retention schedules; federal program rules for HHS, tax, and public safety data	Law and regulation	Vital records, property, courts, tax, HHS, elections	Set confidentiality and verification horizons in the QASI from the schedule
Election system certification	EAC voluntary voting system guidelines; state certification authorities	Regulation where adopted by the state	Election management, voter registration, results transmission	Raise PQC requirements through certification bodies as well as vendors (section 9)

3. Citizen data horizons and HNDL exposure

3.1 Why government data presents elevated HNDL risk

Government entities hold some of the longest-lived sensitive data of any sector. Property records, vital statistics, court records, and tax records are maintained for generations — not years. An adversary who harvests encrypted government data today may find it fully readable within the retention and use period of that data. This makes harvest-now, decrypt-later not a theoretical future concern but a present operational exposure for government entities holding long-lived citizen records. QCI-QS1 v2.3 records the obligation as a confidentiality horizon, and separately as a verification horizon where the record must remain provably authentic — which for property, court and vital records is the whole point (QCI-5.2-01).

Government data type	Typical retention	HNDL risk level	Rationale
Vital records (birth, death, marriage)	Permanent	High	Permanent retention combined with identity value makes this a primary harvest target with no expiry window; verification horizon is also permanent

Government data type	Typical retention	HNDL risk level	Rationale
Property and land records	Permanent to 50-plus years	High	Property ownership records are legally authoritative documents; compromise creates fraud and chain-of-title risks, so signature verification matters as much as confidentiality
Court records and criminal history	Permanent for felony; 7 to 25 years for other offenses	High	Sensitive individual data with long retention; sealed or expunged records carry additional legal sensitivity
Tax and revenue records	7 to 10 years minimum; longer for audit purposes	High	Financial data with fraud and identity theft value; interoperability with federal systems increases exposure and brings the EO 14412 dates closer
Health and human services records	Varies; often 7 to 20 years	High	May include sensitive health, benefit, and family information; often subject to state confidentiality statutes beyond federal HIPAA requirements
Election records and voter data	Varies by state; often 2 to 22 years	High	Voter registration data is both sensitive and a target for state-actor interference; election system integrity is a national security concern
Public safety records (arrest, incident)	5 to 20-plus years	Medium to High	Law enforcement operational data; compromise affects both individual privacy and investigative integrity
Licensing and professional certification	Duration of license plus 7 years minimum	Medium	Credential fraud potential; interconnected with federal databases in many licensing categories

3.2 The legacy system HNDL compounding problem

Government HNDL exposure is amplified by a characteristic unique to this sector: systems that were deployed 15 or 20 years ago are still in production, using cryptographic configurations that have never been updated, protecting data that must remain confidential for decades to come. The combination of old crypto, long retention, and limited upgrade capacity creates a compounding exposure that grows with each year the system remains in production without a migration plan.

When completing the QASI for government systems, practitioners and IT teams should apply this compounding lens: the exposure assessment should reflect not just today's exposure but the cumulative exposure created by the expected remaining system lifetime. A system that will remain in production for another 10 years, protecting data with a 20-year retention obligation, using cryptographic algorithms deployed in 2010, is a materially different risk profile than the individual fields in the QASI suggest when read in isolation. QCI-4.2-02 asks for exactly these factors — horizons, present capture exposure, lead time, end-of-support and applicable deadlines — in every roadmap decision.

4. Procurement cycles and legacy system constraints

4.1 Why government procurement creates unique quantum risk

Government procurement is the single most important contextual factor distinguishing quantum readiness in this sector from every other sector QCI works with. In private sector organizations, a decision to replace or upgrade a system can be made and executed within months. In government, the same decision may require a legislative appropriation, a competitive procurement process lasting 12 to 24 months, a contract award and protest period, and a multi-year implementation. The total timeline from decision to deployment can exceed five years.

This means that quantum readiness decisions made today will not produce deployed solutions until 2030 or later. Systems being procured in 2026 will be in production in 2028 and expected to remain in service until 2038 or beyond — well within the timeline where quantum computers capable of breaking current encryption are projected to be operational, and past every federal deadline in section 2.1. Government entities that do not include PQC requirements in procurement documents being written today are procuring systems that will be quantum-vulnerable from the day they go live.

4.2 PQC requirements in procurement documents

The most high-leverage action available to any state or local government entity is inserting post-quantum cryptography requirements into technology procurement documents before contracts are signed. QCI-7.1-02 requires new or renewed material procurements to evaluate PQC profiles, migration support, upgrade cost and lead time, evidence access, support life, change notification, and exit options. The following language is suitable for inclusion in RFPs, RFIs, and contract terms for technology systems handling sensitive citizen data:

Model procurement language: post-quantum cryptography readiness

The vendor shall provide a written post-quantum cryptography (PQC) migration roadmap for all cryptographic functions in the proposed solution, including TLS, data encryption at rest and the protection of its keys, digital signatures, key establishment, and identity authentication. The roadmap shall reference NIST FIPS 203, 204, and 205 and shall include dated milestones, by product release, for the approved cryptographic profiles the solution will support, whether hybrid or PQC-only, with the construction and fallback behaviour of any hybrid profile specified. The vendor shall complete the contracting agency's supplier request (QCI-QS1 Annex C) and provide an attestation signed by an officer on the agency's form, refreshed annually and on material cryptographic change, and shall notify the agency of any material change to the roadmap within 30 days. The vendor shall provide a scoped cryptographic bill of materials for the solution meeting the agency's evidence requirements. Failure to provide a roadmap or attestation, or material deviation from committed milestones, shall constitute a performance issue subject to the contract's remediation provisions.

Entities that cannot insert PQC requirements into current procurement cycles should at minimum add the following to vendor evaluation criteria: whether the vendor has published a PQC roadmap referencing NIST standards, and whether the vendor can provide a written, officer-signed attestation of its current cryptographic posture and migration timeline. A vendor who cannot answer these questions in a 2027 procurement should receive a lower technical evaluation score than one who can.

4.3 Legacy system migration sequencing

For systems already under contract or beyond the point where procurement terms can be modified, the following sequencing guidance applies. It is a risk and lead-time decision under QCI-4.2-02, not a fixed order:

- Identify systems with both long confidentiality or verification horizons and long expected remaining service life first. These carry the highest compounding HNDL risk and should be the top remediation targets regardless of technical difficulty.
- Separate the vendor migration question from the agency migration question. Some cryptographic upgrades require vendor action. Others — certificate rotation, TLS configuration, API authentication changes — can be performed by agency IT teams independent of the platform vendor. Identify and execute agency-controlled upgrades first to demonstrate progress and build crypto agility competency; one of them, tested under QCI-4.7 on a critical pathway, is what passes gate G80.
- Use contract renewal windows as migration forcing functions. Every contract renewal is an opportunity to insert PQC requirements, request vendor attestations, and establish migration milestones as performance metrics. Track contract renewal dates for all critical system vendors and prepare quantum readiness requirements six months before each renewal.
- For systems with no near-term upgrade path, implement compensating controls and document them explicitly. A system that cannot be migrated in the next five years should have documented compensating controls — data minimization, enhanced access logging, network segmentation — and a formal exception under QCI-4.3-02 with an expiry, review triggers, and the documented reason no exit is feasible. The exception is managed; it does not clear the exposure flag (QCI-5.3-01) and it does not lift gate G70.

4.4 Long-lead trust and hardware decisions

QCI-4.2-02 forbids a roadmap that postpones all signature, trust-anchor and hardware work until key-exchange work is complete. In government the long-lead items are the ones with the longest procurement cycles: PKI roots and trust stores used across agencies, public safety radio and device fleets, and election equipment. Start those decisions when the lead-time analysis requires, in parallel with the transit work that closes present-tense harvest exposure.

4.5 What gate G70 means for government entities

Under QCI-QS1 v2.3, an organization cannot score above 70 until every critical supplier has provided a current, adequate response and an officer-signed attestation (gate G70, QCI-6.3-01). An approved exception, however well managed, does not lift the cap. For a government entity that is the rule with the sharpest edge: the enterprise resource planning platform, the citizen portal, the identity provider, the managed service provider, and the election system vendor are each critical suppliers, and any one of them unattested holds the score at 70.

That is the rule working as designed. The entity cannot fix the vendor’s cryptography, and the standard does not pretend it can; it moves the pressure to the vendor, and in government the entity has the strongest lever of any sector: the procurement document. Section 4.2’s model language makes the attestation a contract deliverable. An entity that has done everything in its own power and is held at 70 by an unattested vendor has a defensible position with auditors, legislators, and grant reviewers, and the exception register is the evidence. An entity that reports 74 with an unattested ERP vendor has a finding.

5. QASI record guidance for government entities

The following guidance supplements the QASI record groups in QCI-5.2-01. A field may hold a known value, an explicit unknown with an investigation action, owner and due date, or a justified not-applicable value (QCI-5.1-02). For a legacy system whose vendor cannot say what it uses, “unknown — vendor asked [date], due [date]” is the honest entry, and the record stays outside validated coverage until it is resolved.

QASI field	Government-specific guidance
Business criticality	Election systems: always High regardless of scale. Vital records, property records, public safety: High. Revenue and tax systems: High. Licensing systems: Medium to High depending on federal interconnection. Internal HR systems with no citizen data: Low. Criticality follows QCI-1.1-02: a system or flow whose failure could exceed approved risk appetite is critical.
System owner and technical reviewer	For government systems, name both the technical owner (IT director or system administrator) and the business owner (agency director or department head), and the technical reviewer who validates the record. All are required because quantum risk decisions in government require both technical execution and administrative authorization, and validation needs a reviewer (QCI-5.1-02).
Confidentiality and verification horizons	Use permanent for vital records and property records, for both horizons. Calculate from current citizen ages for records with age-based retention (juvenile records, benefit records). When state law specifies a retention period, use the longer of the legal minimum and the practical need.
Critical data flows	New in v2.3: flows are a separate coverage denominator (QCI-5.1-03). Inventory at minimum: federal data exchanges (tax, HHS, public safety), citizen portal to back-office, payment processing, inter-agency identity federation, and results transmission for elections, with protection and authentication at each hop.
Vendor dependencies	Name the platform vendor and the state or county IT service provider separately, with product and deployed release. Many government entities receive IT services through a shared services arrangement or a managed service provider — both the platform vendor and the service provider are critical suppliers under QCI-7.1-01, and both must attest for G70.
PQC support status	Expect None for most legacy government platforms. Distinguish supported, configured and observed (QCI-4.5-01). Do not accept general security certifications (FedRAMP, StateRAMP) as evidence of PQC readiness — these certifications do not currently address post-quantum cryptography, and under QCI-4.8-03 they are recorded as supplier assertions or module validations, never as system acceptance.
Crypto agility status	Government systems almost universally have None or Partial crypto agility due to legacy architecture and vendor dependency. Document this limitation explicitly rather than leaving the field blank. A documented None with a contract renewal date is more useful than a blank field.
Exposure flags	Apply the compounding lens from section 3.2. For systems with long expected remaining service life protecting data with long horizons under vulnerable protection, raise the long-lived-confidentiality flag and, for authoritative records, the long-verification-horizon flag (QCI-5.3-01). Treatment status is recorded separately; a contract renewal date is a milestone, not treatment.

QASI field	Government-specific guidance
Target remediation date	For government systems, the target remediation date should be the earliest of the next contract renewal date, any applicable federal or grant deadline from the obligations register, and the projected date when quantum computers capable of breaking current algorithms are expected to be operational. All constraints should be noted, by milestone type (planning, procurement, pilot, acceptance, retirement) per QCI-4.2-02.

6. Governance model for government entities

6.1 State-level governance

State-level quantum readiness governance maps naturally to the existing state cybersecurity governance structure. Most states have a designated CISO with authority over state agency information security programs. Adding quantum readiness as a mandate within that existing authority structure is more efficient than creating parallel governance, and QCI-4.2-01 permits the records to live in existing management systems:

QCI-QS1 required role	State government mapping	Minimum commitment
Executive Sponsor	State CISO or CIO — whoever has cross-agency information security authority	Quarterly briefing to the governor's office or cabinet IT committee; annual legislative technology committee briefing; approval of the assessment boundary
Quantum Risk Owner	Deputy CISO or senior security architect within the state cybersecurity office	Monthly program coordination; quarterly Q-Risk Score production and obligations register review; annual QASI refresh
Steering function (risk committee)	Existing IT security council or agency CIO council; add quantum risk as a standing agenda item	Quarterly: agency Q-Risk Score review, vendor exception register, migration roadmap milestones
Governing body	Governor's office, cabinet, or legislative technology committee — depending on state governance structure	Annual briefing minimum; semi-annual if the quantum risk rating is High; explicit approval of any accepted risk (QCI-8.2-01)
Procurement and vendor risk	State procurement office and agency contract managers	As needed: PQC language in RFPs, Annex C issuance with 60-day deadlines, attestation tracking, contract renewal quantum requirements

6.2 County and municipal governance

County and municipal governments face a staffing reality that state agencies often do not: many have a single IT director who handles everything from network maintenance to cybersecurity to help desk. The governance model for these entities must be achievable with minimal dedicated staff:

- Executive sponsor: County administrator, city manager, or mayor — whoever approves the IT budget. The sponsor does not need technical expertise. They need to understand that quantum risk is a documented threat with a measurable program response, and they need to authorize the Quantum Risk Owner to act.
- Quantum Risk Owner: IT Director or the most senior IT staff member. For counties and municipalities using a managed service provider, the MSP security lead can co-own this role if the contract supports it — but a named government employee must retain accountability, and the MSP is itself a critical supplier that must attest.
- Governing body briefing: County commission, city council, or board of supervisors — the governing body in the standard's terms (Clause 3). Quarterly briefing using the governing-body insert format from QCI-QS1 Annex D. Most elected governing bodies will respond better to the citizen data and HNDL framing than to technical cryptography language.

7. Q-Risk Score guidance for government entities

7.1 Realistic band targets by government tier

QCI-QS1 defines score bands from Exposed (0 to 19) through Defensible readiness (81 to 100). A score of exactly 80 is Advancing, and no score above 80 is possible unless gates G60, G70 and G80 have all passed (QCI-6.3-01, QCI-6.5-01). The targets below are planning guidance for this sector, not Core-profile thresholds (QCI-6.3-02). None reaches 70, and none could while any critical vendor or service provider is unattested.

Government tier	Typical starting score	Realistic 12-month target	Primary constraint
State agency with dedicated security team	14 to 26	38 to 55 (Behind to Mobilizing)	Legacy platform vendor timelines; procurement cycle for migration
State agency, shared IT services	8 to 18	28 to 44 (Behind to Mobilizing)	Shared service provider quantum readiness; cross-agency coordination overhead
County government, 100K-plus population	6 to 16	24 to 38 (Behind)	Limited dedicated security staff; legacy system dependencies
County government, under 100K population	3 to 10	18 to 30 (Exposed to Behind)	Single IT generalist; no dedicated security function; MSP dependency
Municipal government, large city	10 to 22	32 to 48 (Behind to Mobilizing)	Multiple department siloes; varied vendor estates; procurement complexity
Municipal government, small to mid city	4 to 12	20 to 34 (Behind)	Limited resources; high MSP and platform vendor dependency

Scoring honestly in a resource-constrained environment

Government entities often resist producing a low Q-Risk Score because they fear the political optics of a low number appearing in an audit or a public records request. The correct response to this concern

is that a low score with a documented improvement plan is a governance success, not a governance failure. It demonstrates that the entity identified a risk, measured it accurately, and is managing it. An undocumented risk that surfaces in an incident is the governance failure. The score is reported with its assessment type, self-assessment or independent assessment (QCI-1.2-03), and with conformance status beside it rather than inside it (QCI-1.2-04); a public records request that produces an honest, labelled number is a better outcome than one that produces an inflated one. Help government clients understand this framing before producing their first score.

7.2 The procurement readiness note

Earlier editions of this supplement suggested scoring a procurement readiness dimension separately as a government-specific addendum to P4. Under QCI-6.3-02, organization-specific dimensions may be reported only as separately named supplemental metrics, never as part of the Core score. Keep the note: record, beside the P4 level, the number of critical systems whose next procurement or renewal includes the section 4.2 requirements, and the number that do not. It is the most useful single indicator of whether the entity is buying its way out of the problem or into it. Label it “procurement readiness, supplemental” and never fold it into the score.

8. Government entity 90-day quick start

This sequence adapts the Practitioner Handbook’s establishment sequence and QCI-QS1 Clause 9.1 for a government entity. It is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Week 1	Assign and bound	Name the executive sponsor and Quantum Risk Owner. Declare the assessment boundary (QCI-1.1-01): which systems and flows are in scope for the initial QASI. For state agencies, start with systems that interoperate with federal systems — these face the earliest PQC alignment requirements under EO 14412. Seed the obligations register from section 2.4.	Written role assignment. Approved boundary with critical systems list. Obligations register started. Added to the information security program.
Week 2	Procurement review	Review all active RFPs and contracts in the procurement pipeline. Insert the section 4.2 requirements into any RFPs not yet finalized. Flag upcoming contract renewals for PQC requirement insertion.	PQC language added to open RFPs. Contract renewal calendar with quantum readiness flags for the next 24 months.
Weeks 3 to 4	Vendor requests	Issue Annex C requests to the three most critical system vendors and to the managed service provider where one operates the estate. For government entities, the vendors are typically the enterprise resource planning platform, the citizen portal or digital services platform, and the identity and access management system.	Requests issued with a 60-day response deadline (QCI-7.2-04). Logged in the vendor management record.

Timeframe	Phase	What to accomplish	Output
Weeks 5 to 7	QASI build	Build linked QASI records for the five highest-criticality systems and the critical flows between them and to federal exchanges, using the field guidance in section 5. Apply the compounding HNDL lens from section 3.2. Validate each record with the named owner and a technical reviewer; record unknowns explicitly.	Five system records and their flows completed and validated. Compounding exposure documented for long-tenure systems.
Weeks 8 to 9	Expand and flag	Extend the QASI to remaining critical systems and flows toward the 95 percent threshold. Identify all systems with no vendor PQC roadmap and long remaining service life. These are the exception register candidates.	Coverage computed per QCI-5.1-03 for systems and flows. Top 10 remediation targets identified. Exception register opened under QCI-4.3-02 for systems with no near-term migration path.
Week 10	Score	Produce the first Q-Risk Score using the Annex B worksheet and the QCI-6.1-02 formula. Record the assessment type. Apply the government band targets from section 7 as planning context. Record the procurement readiness note as a supplemental metric.	Self-assessed Q-Risk Score snapshot with gate results and evidence links. Procurement readiness note appended, labelled supplemental.
Weeks 11 to 12	Brief and plan	Deliver the governing-body insert (QCI-8.1-01). Frame the program as citizen data protection and civic responsibility. Prepare SLCGP documentation if a grant application is in scope. Start the roadmap with milestone types per QCI-4.2-02, including the long-lead trust and hardware decisions.	Governing-body briefing delivered. SLCGP documentation prepared if applicable. PQC migration roadmap draft begun.

9. Election system quantum readiness addendum

Election systems represent a special case within government quantum readiness. They are both among the highest-consequence systems for cryptographic compromise — election integrity is a fundamental democratic function — and among the most complex to upgrade, given the involvement of election officials, voting system certification processes, and federal and state election law.

- Treat all election systems as High business criticality with permanent verification horizons in the QASI, regardless of the specific function. Authentication to election management systems, ballot tracking and chain-of-custody signing, voter registration database protection, and results transmission all carry cryptographic exposure with direct democratic integrity implications. The exposure here is mostly authenticity, not confidentiality: the question is whether a result or a record can be forged, which is the verification horizon.
- Election system vendors (Dominion, ES&S, Hart InterCivic, Unisys) operate under voting system certification processes that are separate from normal IT procurement. PQC requirements need to be raised through both the vendor engagement process and the relevant federal and state certification bodies, including the EAC and state certification authorities. Certification of equipment is a supplier assertion or module validation under QCI-4.8-03; it is not evidence that the deployed configuration is post-quantum.
- The timing sensitivity of election systems creates an additional constraint: cryptographic upgrades cannot be deployed during active election periods. Migration planning must

account for election calendars and the limited windows available for system changes, which makes the long-lead planning of QCI-4.2-02 mandatory rather than advisable.
- State election directors and county clerks are the governing authority for election systems, not IT departments. Quantum readiness engagement for election systems must include election officials, not just IT staff.

Election system quantum risk is a national security matter

Nation-state adversaries are among the most capable and motivated actors in the harvest-now, decrypt-later threat landscape, and for election systems the nearer threat is forgery rather than decryption. Election systems are among their highest-value targets. A state that cannot demonstrate the cryptographic integrity of its election systems is not just facing an IT risk — it is facing a sovereignty risk. State election directors and governors should understand quantum readiness for election systems in this context.

10. Summary and engagement

State and local government entities hold the citizen data that underlies identity, property, public safety, and democratic participation. The cryptographic infrastructure protecting that data is aging, vendor-dependent, and operating under procurement constraints that make rapid migration impossible. The organizations that begin planning now — before procurement documents are finalized, before contracts are renewed, before legislative technology committees begin asking questions — will be the ones in control of their own migration timeline.

The organizations that wait will find themselves migrating under pressure, at cost, on someone else's schedule. Since June 2026 that schedule has federal dates on it. In government, that pressure arrives as examination findings, legislative hearings, and eventually constituent harm. None of those outcomes are necessary. They are the predictable result of treating a long-horizon risk as someone else's future problem.

QCI engagement support for state and local government

QCI works with state agencies, county governments, and municipal authorities to deliver calibrated QCI-QS1 assessments, support SLCGP grant documentation, develop procurement language for RFPs and contract renewals, and prepare governing-body briefings that translate quantum risk into the language of civic responsibility and constituent protection. Independent assessment under QCI-1.2-03 is available separately. Contact QCI to discuss how an engagement is scoped for your government tier and resource level.

Revision history

Version	Date	Changes
1.2	September 23, 2026	Aligned to QCI-QS1 v2.3: references by requirement identifier; federal policy table rewritten for EO 14412 and OMB M-26-15 (M-23-02 superseded; EO 14028 retained as context); obligations register section 2.4 added; band targets restated for the 81-point Defensible readiness threshold; gate G70 no longer satisfied by exceptions (new section 4.5); G60 fixed at 95 percent for systems and flows, with critical-flow guidance; horizons replace data longevity, with verification horizons for authoritative and election records; model procurement language extended to the Annex C attestation and CBOM; long-lead decisions section 4.4 added; procurement readiness recast as a supplemental metric (7.2); governing-body terminology.

Version	Date	Changes
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).