

NSW Government Transition to Post-Quantum Cryptographic Cyber Security - Expert Advice

Terms of Reference (ToR)

1. Background

The Government Chief Information and Digital Officer (GCIDO) is seeking independent expert advice on the actions NSW Government should take between now (2026) and 2030 to prepare for the transition to post-quantum cryptography (PQC), including planning, prioritisation and sequencing across NSW Government systems and services.

Cryptographically relevant quantum computers (CRQCs) are expected to undermine current traditional cryptography. The migration to PQC is a large-scale technology effort that will take several years. The Australian Signals Directorate (ASD) advises organisations to plan now to transition away from traditional asymmetric cryptography by end-2030.¹ Similar work is underway in Five Eyes nations (including the United States,^{2,3} United Kingdom⁴ and Canada⁵) to transition to PQC over the next 5-10 years.

An Expert Panel (the Panel) will be convened to inform the advice and ensure it is aligned with Australian Government advice and international standards and best practice.

The Panel will be chaired by the NSW Deputy Chief Scientist & Engineer and supported by the Office of the NSW Chief Scientist & Engineer (OCSE). The Panel will comprise a minimum of four Members with expertise in areas post-quantum cryptography, quantum algorithms, quantum computing, cyber security, standards government IT procurement and information systems.

3. Scope and Deliverables

The OCSE, in consultation with the Department of Customer Service, will convene a technical panel of relevant experts to address the following (NB: specific example questions to guide panel deliberations is provided in Appendix 2):

¹ Australian Signals Directorate, *Information Security Manual* (March 2026), available at: www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism.

² United States Cybersecurity & Infrastructure Security Agency, *Post-Quantum Considerations for Operational Technology* (October 2024), available at: www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology.

³ United States National Institute of Standards and Technology, *Transition to Post-Quantum Cryptography Standards* (November 2024), available at: <https://doi.org/10.6028/NIST.IR.8547.ipd>.

⁴ United Kingdom National Cyber Security Centre, *Timeline for migration to post-quantum cryptography* (March 2025), available at: www.ncsc.gov.uk/guidance/pqc-migration-timelines.

⁵ Canadian Centre for Cyber Security, *Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)* (June 2025), available at: www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001.

1. The potential implications, scale and timing of quantum computing advancements - particularly cryptographically relevant quantum computers (CRQCs) - for NSW Government cyber security, service delivery, and operational resilience.
2. Which NSW Government systems, services and information assets are of highest priority for protection, and determining the criteria for prioritisation based on risk, criticality, and potential impact.
3. What a successful transition to PQC would look like for the NSW Government, including key outcomes, migration pathways, sequencing, and milestones.
4. Recommending governance, coordination, and resource allocation strategies to support an effective and timely government-wide response to quantum-related cyber risks.
5. Approaches for identifying and managing risks associated with third-party systems, service providers and supply-chain dependencies as the NSW Government transitions to PQC.
6. Mechanisms for collaborating and aligning with the Australian Government, other jurisdictions, standards bodies, and international best practice throughout the PQC transition.

The Panel's advice will be confined to select group of cases studies of NSW Government systems and services delivered directly by a NSW Government agency or procured by Government from third-party IT providers (including contracted cloud and managed services). These case studies will be agreed by the Chief Scientist, GCIDO and relevant accountable agency head, and will be de-identified as part of the final report. Advice may be extended to consider critical supplier dependencies and broader critical infrastructure interoperability impacted by CRQCs. Informed by these case studies, the Panel's advice will pertain to a framework and systems that can be adopted across all NSW Government entities.

The Panel will **not**:

- perform system-by-system audits.
- be responsible for implementing changes.
- recommend third party technology providers used by the NSW Government.

Report

The OCSE will produce a report to the Minister for Customer and Digital and the Department of Customer Service (DCS) setting out their advice and recommendations in response to this TOR within 8 months of Ministerial authority being received. The final report will be publicly available on the OCSE website.

NOTE: Information that poses an unacceptable risk to the security and integrity of NSW Government systems may be redacted from the final report before it is made publicly available, by agreement of the NSW Chief Scientist and Government Chief Information and Digital Officer, in consultation with the NSW Chief Cyber Security Officer.

Appendix 1: Expert Panel Arrangements

Composition and size

- The Panel will comprise a minimum of four Members with expertise in areas post-quantum cryptography, quantum algorithms, quantum computing, cyber security, standards government IT procurement and information systems.
- Panel Members will be appointed by the NSW Chief Scientist & Engineer (Premier's Department) in consultation with the Government Chief Information and Digital Officer (DCS).
- The Panel will be chaired by the NSW Deputy Chief Scientist & Engineer.
- The OCSE will provide Secretariat support to the Panel including in drafting of the report and executive summary.

Role and responsibilities of the Chair

The Chair is responsible for leading the activities of the Expert Panel including:

- Ensuring that the Expert Panel performs its functions, acting within any relevant statutory powers, legal obligations and complying with policies.
- Facilitating the conduct of meetings to allow frank and open discussion.
- Facilitating the flow of information to members and stakeholders.
- Liaising with the Secretariat and NSW Government executives.

Role and responsibilities of Panel Members

Members are expected to:

- Support the functions of the Expert Panel.
- Provide analysis and expertise to inform decision making.
- Review data and information to provide feedback to the NSW Government.
- Attend meetings and participate in discussions.
- Undertake consultation or research and review relevant materials prior to meetings to facilitate discussion of the agenda items.

4. Meetings

The Secretariat will coordinate Expert Panel meeting times and locations in consultation with the Panel Members.

5. Secretariat

Primary secretariat support for the Expert Panel will be provided by the OCSE. When required, additional support may also be provided by DCS.

Secretariat support will include:

- Administration including agendas, papers, and minutes.
- Logistics including pre-briefs, meetings, and workshops.

- Coordination with NSW Government agencies and external stakeholders.
 - Report drafting.
-

6. Quorum

A quorum is constituted by the Chair and at least half of the Expert Panel members. No findings or recommendations may be made in the absence of a quorum.

7. Code of Conduct

Declaring pecuniary and conflicts of interests

The Chair and Panel Members must declare actual or perceived conflicts of interest, and pecuniary interests upon their appointment, and advise the Secretariat accordingly if there are any updates for the duration of their tenure.

Managing conflicts of interests

The Chair and Panel Members must:

- Disclose any actual or perceived conflicts of interest which may exist as soon as they become aware.
- Declare any actual or perceived conflicts of interest at the start of each relevant meeting.
- Comply with any conflict of interest management actions as directed by the Chair or Secretariat.

Confidentiality

Any business transacted in Expert Panel meetings including deliberations, findings, decisions, conclusions, and proposed recommendations is strictly confidential unless otherwise stated.

8. Consultation and access to information

- Where appropriate and necessary, the Secretariat and DCS will facilitate the Expert Panel having access to NSW Government stakeholders and information subject to appropriate confidentiality controls.
 - Additional procedures regarding confidentiality may be required for access to state sensitive information.
 - The Panel may consult with select non-governmental experts with the approval of the Secretariat and consultation with DCS
-

9. Decision Making

- (a) The Chair is responsible for the escalation of any issues from the Expert Panel to the Chief Scientist & Engineer (Premier's Department).
- (b) The Chair may provide advice on behalf of the Expert Panel where majority but consensus is not reached. Where this is appropriate, the Chair is required to represent dissenting views.

Appendix 2: Panel Advisory Questions

Example questions to guide panel deliberations are provided below. This list is not exhaustive, and the Panel may address other topics deemed necessary to address the Terms of Reference.

1. What is the nature, scale and timing of the quantum risk to NSW Government cyber security, service delivery and operations?

- a. How are CRQCs expected to affect the confidentiality, integrity and security of NSW Government information, systems and services?
- b. Over what timeframes are these risks expected to emerge?
- c. Which classes of NSW Government digital and physical systems are likely to be most vulnerable to quantum-related cyber risk?

2. What should the NSW Government protect first and why?

- d. Which NSW Government systems, services and information assets are the highest priority for protection? This analysis could include a standard classification of system risk.
- e. What factors should determine priority?

3. What would a NSW Government transition to PQC look like?

- a. What outcomes should NSW Government aim to achieve in response to quantum-related cyber risks?
- b. What planning, sequencing and milestones are required to migrate to PQC?
- c. What additional protective measures, beyond migration to PQC, should the NSW Government consider?

4. How should the NSW Government organise and resource its response?

- a. How should the NSW Government allocate effort and resources across agencies, systems and service environments?
- b. What governance, oversight and coordination arrangements are required?
- c. What key decisions need to be taken early to enable an orderly and timely transition?

5. How should the NSW Government manage third-party and supplier risk?

- a. What third-party systems, services and supply-chain dependencies relied on by the NSW Government are vulnerable to CRQCs?
- b. How should NSW Government manage these risks, including through procurement, assurance, standards, contracting and vendor engagement?
- c. How should NSW Government engage critical infrastructure providers and technology partners on PQC?

6. How should NSW Government work with other governments and external bodies?

- a. How should NSW Government align its response with Australian Government advice, relevant standards and international best practice on PQC?
- b. How should NSW Government engage with the Australian Government, standards bodies and other relevant jurisdictions on PQC?