Quantum Resilience in the Australian National Security Legislative Framework[1]

Authors:

Susanne Lloyd-Jones[2]

Kayleen Manwaring[3]

September 2024

[1] **Acknowledgements:** Thanks to Jennifer Westmorland for her research assistance and assistance in developing the content of this brief. Thanks also to the research assistants and interns of the UNSW Allens Hub for Technology, Law & Innovation: Catherine Nguyen, Annabelle Lee, Megha Uppal and Natarsha Wong. Thanks also to those who provided helpful comments and suggestions, in particular Lyria Bennett Moses, Warren Armstrong, Praveen Gauravaram, Barry Bazara and Rachel Mahncke. The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme. In 2018, the CSCRC was awarded $50 million in Commonwealth funding over seven years. This funding is supplemented by contributions from industry, university, and government agency Participants.

[2] Cyber Security Cooperative Research Centre Postdoctoral Fellow.

[3] Associate Professor, UNSW Law & Justice.

Contents

Executive summary

The advent of quantum technology applications presents a significant challenge to cybersecurity worldwide, with the potential to compromise classical cryptographic systems.[4] This policy brief focuses on Australia's preparedness in the face of evolving quantum technology applications, acknowledging the heavy reliance on cryptographic techniques and the predicted future risk of quantum-enabled capabilities including decryption and signature forgery. While quantum-resilient cryptography shows promise, policy tensions arise between the necessity for continuous research and innovation, the requirements of security stakeholders and the imperative to safeguard privacy and security of data.

The brief explores the potential of quantum computers to undermine the effectiveness of current cryptographic processes and infrastructure, emphasising the need to develop quantum-resilient cryptographic methods, processes and technology, such as quantum key distribution (QKD) and post-quantum cryptography (PQC). However, it also investigates a consequent tension arising between ensuring privacy of communications and enabling law enforcement agencies to intercept communications for investigative purposes.

This brief analyses Australia's National Quantum Strategy and Cyber Security Strategy, highlighting commitments to quantum development and the need for post-quantum cryptography standards. The *Security of Critical Infrastructure Act 2018* (Cth) (SOCI), Part 14 and Part 15 of the *Telecommunications Act 1997* (Cth) (TA) and Part 5-3 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) are discussed, emphasising the tension between innovation, security obligations and the use of strong cryptography. We note that technological progress of software techniques and traditional computing at present are likely to impact cryptographic security more than near-term quantum specific developments. However, this brief explores national and international approaches to cryptographic resilience in the context of emerging quantum technologies. [5]

The brief outlines the approaches of the European Union, India, the United Kingdom, and the United States, providing insights into their legislative frameworks, key legislation relevant to quantum technologies, and standards development efforts. It highlights the complex policy landscape surrounding quantum technologies and cryptographic methods and processes including public-key encryption, digital signatures, and key-exchange protocols.

Serving as a foundation for further research and policy development, the brief recognises the need for a nuanced and adaptive approach to address the evolving challenges posed by quantum advancements.

Recommendations

1. *Design adaptable quantum resilient regulation for the short, medium and long term*

2. *Incorporate quantum standards into existing frameworks*

---

[4] Michele Mosca, 'A quantum of prevention for our cybersecurity', *Global Risk Institute* (Report, 5 September 2016) < https://globalriskinstitute.org/publication/quantum-computing-cybersecurity/> 1.

[5] We acknowledge some researchers regard some of the predictions about the impact of quantum information science as scientific hype. See eg, Olivier Ezratty, 'Mitigating the quantum hype' ArXiv.org (Web Page, 23 January 2022) https://arxiv.org/abs/2202.01925; Frank Smith, 'Quantum technology hype and national security' 51(5) *Security Dialogue* 488-516; Ernst and Young, *Beyond the Hype: A Critical Look at Quantum Computing's Potential for Business and Society in Asia-Pacific* (Report, 2023).

3. *Contribute more funding for Australian quantum-resilient development*
4. *Continue to advocate for standards development*
5. *Explore law enforcement capabilities*
6. *Develop the Australian Public Service into a quantum workforce, capable of supporting the government's goals*
7. *Contribute to better understanding of the impact of quantum computing on other emerging technologies and associated risks*
8. *Promote collaboration and partnerships between public, private and research sectors to enable development and utilisation of tools for easier access and testing*
9. *Establish resilient quantum supply chain following a risk-based approach*
10. *Develop guidelines for users and vendors of quantum computing solutions (e.g., hardware requirements and impact on performance)*

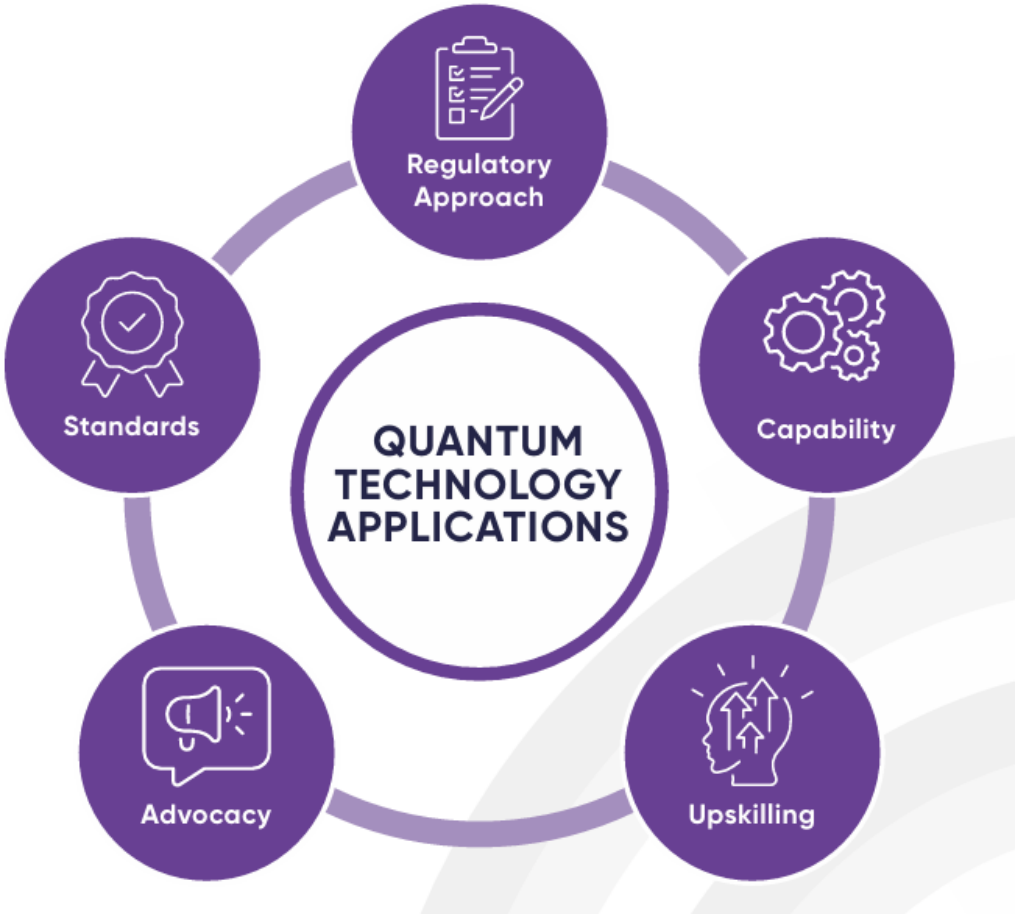

Figure 1: Recommendation for coordinated implementation of regulatory and policy approaches[6]

[6] Figure 1 copyright belongs to the Cyber Security Cooperative Research Centre Ltd.

1 Introduction

A developing quantum industry brings significant advantages and risks for cyber security of systems, networks, and infrastructure. In Australia and worldwide, cryptographic technologies are currently essential to secure a range of network and data transactions and functions. There exist concerns that potential heightened computational power in high-functioning quantum computing could be applied by malicious actors to break contemporary cryptosystems, such as encryption algorithms, public key digital signatures, key exchange protocols and public key infrastructure, that are resistant to conventional computing power. This ability could enable successful cyber-attacks on governments, businesses, and individuals.[7] While quantum computing developments have not yet achieved this capability,[8] there is apprehension that cyber-attacks *in the present,* for example, on encrypted data will increase *in anticipation* of quantum decryption capabilities ('pre-quantum'). Identified as the 'harvest now, decrypt later' problem, it is a method where encrypted data is stolen and stored for future decryption by a computer with sufficient power, which is predicted to be a quantum computer. The problem will impact asymmetric cryptography due to the transmission of data and public keys.[9]

Technical developments in quantum-resilient encryption[10] and innovation in quantum communications hold some promise in defending against these attacks. However, law enforcement and national security stakeholders have policy drivers towards communication interception and decryption that may conflict with encouraging government support of these technologies.

This document provides a brief introduction to the policy and legal support and barriers to quantum-resilient cryptographic systems in Australia, and an overview of approaches in the US, UK, EU and India. It is intended to assist in gauging Australia's regulatory preparedness for quantum, acknowledging the policy tension and technology gaps that exist. The issues are complex, and could not be comprehensively covered due to project constraints, but provides several guideposts towards further research and policy development in this area.

The policy options set out in section 3 are recommended based on our analysis of existing best practice approaches internationally and the gaps we have observed in Australian and international approaches.

2 Policy options

2.1 Reconciling competing goals

Given the significant cyber security challenges the emergence of quantum technologies presents, there is a need to reconcile competing policy and regulatory goals around quantum-safe encryption. Key steps to achieving such goals are explored below.

a) *Commence* the groundwork for a flexible, proportionate and adaptive regulatory pathway for quantum technology applications for the short, medium and long term. The United

---

[7] Beth Waller and Elaine McCafferty, 'Comment: The Necessary Evolution of State Data Breach Notification Laws: Keeping Pace with New Cyber Threats, Quantum Decryption, and the Rapid Expansion of Technology' (2022) 79(1) *Washington and Lee Law Review* 521.

[8] To the extent this can be known from current available open-source information.

[9] See Michal Krelina, 'The Prospect of Quantum Technologies in Space for Defence and Security' (2023) 65 *Space Policy* 101563. See also, Quintessence Labs, 'Quantum Computing is Coming, But Quantum Risk is Here Now', Quintessence Labs FAQs (Web Document, 2022) https://info.quintessencelabs.com/hubfs/QuintessenceLabs-Quantum-FAQs.pdf.

[10] Note however that quantum-resilient encryption algorithms will still be subject to the current need for strong keys that are kept secure.

States and the United Kingdom have both started laying the foundations for the regulation and governance of quantum technology applications. The United States has enacted a suite of quantum-specific preparedness legislation.[11] The Regulatory Horizons Council of the United Kingdom released its approach to the regulation of quantum technology applications in February 2024.[12] Australia should be looking to harmonise its approach to governance and regulation with like-minded countries, yet also taking into account the nation's specific needs, requirements and interests.[13]

b) *Incorporate* quantum standards when they are available from organisations such as NIST/ETSI with existing standards in the SOCI Act. While the SOCI Act can absorb technological developments and applications of quantum technologies through the critical infrastructure risk management program rules (CIRMPR), without positive obligations to mitigate quantum risks and build quantum resilience, many industries may not consider the risks associated with these technologies;

c) *Contribute* more funding for Australian quantum-resilient development: although Australia currently does some sophisticated quantum research and innovation, especially in the university sector, the funding allocation appears low compared to other countries,[14] and much concentrates on areas other than cyber security and encryption;[15]

d) *Continue* to advocate and fund Australian involvement in standards development at both the international (eg ISO, IEEE) and key national/regional levels (eg NIST, ETSI);

e) *Gather* evidence on how successful Australian law enforcement and national security agencies have been in decrypting intercepted data, ie scope the actual problem they will face in the light of 'impenetrable' communications;

f) *Develop* the Australian Public Service (APS) into a skilled and scalable quantum workforce, able to support the government's goals in properly promoting and regulating quantum industries and applications in Australia. While the *National Quantum Strategy* discusses the support of a skilled and growing quantum workforce in industry and academia, its recommendations do not explicitly include the APS. The APS should be included in Action 3.2, or a similar exercise should be undertaken with due focus on the necessary skills specific to the relevant government departments and agencies, eg regulation, trade promotion, law enforcement and intelligence.[16] Knowledge asymmetries between academia, innovators, industry, regulators and government can be mitigated through education, training and impact and engagement activities, such as

---

[11] See Appendix E for details.
[12] See Regulatory Horizons Council, 'Regulating Quantum Technology Applications' (Report, February 2024) <https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf>.
[13] Australian Government, '2023-2030 Australian Cyber Security Strategy', (*Strategy*, 22 November 2023) https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf ('Cyber Security Strategy').
[14] Note that reliable data on funding is difficult to discover. It is likely that much of the funding by government is secret due to a perception of potential national security risks. Also, many funding announcements relate to a very broad set of quantum applications, and do not clearly differentiate between applications centred on communications security developments and those in other areas of quantum.
[15] See eg in Australia, a substantial amount of funding is allocated to attempts to build quantum computing architectures in silicon and optical platforms at UNSW's Center for Quantum Computation & Communication Technology (CQC2T): <https://www.cqc2t.org/research/>. Note however that CQC2T also has active projects in quantum communications security.
[16] Department of Industry, Science and Resources, 'Theme 3: A skilled and growing quantum workforce', *National Quantum Strategy* (3 May 2023, Australian Government) < https://www.industry.gov.au/publications/national-quantum-strategy/themes-national-quantum-strategy/theme-3-skilled-and-growing-quantum-workforce>.

creating opportunities for knowledge transfer, teaching and learning, professional development and talent acquisition.[17]

2.2 Quantum technologies and encryption

It is commonly suggested that quantum computers, when fully operational, will be able to compromise the security goals of several conventional cryptographic systems including key exchange protocols, encryption, digital signatures, and public-key infrastructure. For example, quantum computing power can be used to decrypt communications encrypted with many popular forms[18] of public key (asymmetric) encryption, the process underpinning most communications infrastructure, networks, and applications. Conversely, the implementation of quantum communications technologies could significantly aid in efforts to keep data, systems and hardware secure, aiding confidentiality and privacy, as developers claim that it will be much more resistant to cyber-attacks than current communications technologies.

Advocates argue that the implementation of 'quantum-resistant' cryptographic systems and quantum communications is essential in protecting entities against successful attacks that use quantum computing to compromise the security of conventional cryptography. However, this potential for 'unbreakable' communications has its natural detractors from a policy perspective. National security and law enforcement agencies, such as the AFP and ASIO, are insistent that they are heavily reliant on interception of decipherable communications for many of their investigative functions.[19] This creates a tension between two estimable policy goals: the goal of preventing anyone but the sender and intended receiver from accessing private communications and the goal of intercepting communications between those intent on criminal acts, including terrorism and other serious offences.

3 Overview of some important current law and policy approaches

3.1 Overview of Australian law and policy

3.1.1 Policy approaches to cyber security and quantum development

Australia's National Quantum Strategy,[20] launched 3 May 2023, includes commitments that the Australian government will:

- 'ensure the growth of Australia's quantum ecosystem supports economic prosperity while safeguarding national well-being';[21] and
- 'champion responsible innovation and the introduction of new standards and regulatory mechanisms where national wellbeing is at risk'.[22]

---

[17] See Johanna Weaver and Sarah O'Connor, *Tending the Tech-Ecosystem: who should be the tech-regulator(s)?* (Report, May 2022, Tech Policy Design Centre) https://techpolicydesign.au/wp-content/uploads/2023/08/Web_TPDC_Tending-Tech-Ecosystem_NO.1_2022_2023-Cover-Update_V2.pdf, 7.
[18] Roger Grimes, *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto* (Wiley, 2019) at Chapter 3 provides a useful list of the most vulnerable cipher algorithms ie ones that rely on 'the integer factorization problem, the discrete logarithm problem, the elliptic-curve discrete logarithm problem, or any other closely related mathematical problems'.
[19] Ian Walden, '"The Sky Is Falling!" – Responses to the "Going Dark" Problem' (2018) 34(4) *Computer Law & Security Review* 901; more recently see Mike Burgess and Reece Kershaw, 'Address to the National Press Club of Australia', *ABC News* (YouTube Video, 24 April 2024) <https://www.youtube.com/watch?v=ysi1aIY4NkU>.
[20] Australian Government, 'National Quantum Strategy' (*Strategy*, 3 May 2023) https://www.industry.gov.au/publications/national-quantum-strategy.
[21] Australian Government, *National Quantum Strategy,* Theme 5: A trusted, ethical and inclusive quantum ecosystem, https://www.industry.gov.au/publications/national-quantum-strategy/themes-national-quantum-strategy/theme-5-trusted-ethical-and-inclusive-quantum-ecosystem
[22] Ibid.

In 2023, the Australian government launched the *2023-30 Australian Cyber Security Strategy*.[23] In this strategy, the government recognised the risk that '[a]dvances in quantum computing could leave contemporary cryptography insecure' and the need to 'anticipate future requirements of encrypted systems'.[24] Part of the so-called 'Shield 10' of the Australian government's Quantum Action Plan (primarily focussed on the public sector) is to '[p]repare for a post-quantum world' by:

> [s]et[ting] standards for post-quantum cryptography by updating guidance within the Information Security Manual. Organisations will also be encouraged to prepare for the post-quantum future by conducting a review of their data holdings and developing a plan to prioritise and protect sensitive and critical data.[25]

The Information Security Manual (ISM) is a public document produced by the Australian Cyber Security Centre and its purpose is 'to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats'.[26]

Australia would benefit from commencing development of its regulatory pathway for a flexible, proportionate, and adaptive framework for quantum resilience. The United States and the United Kingdom have surpassed Australia in this regard. The United States has enacted a suite of quantum-specific preparedness legislation aimed at early adoption of quantum-safe practices and technologies by government departments and agencies.[27] In the United Kingdom in February 2024, the Regulatory Horizons Council released a report on its approach to the regulation of quantum technology applications.[28] The report advocates for a 'pro-innovation' regulatory framework that supports the domestic industry, explores 'application specific' regulation that is adaptable and proportionate and appropriate governance around responsible innocation and research.[29]

Australia should be looking to harmonise its approach to governance and regulation with like-minded countries, yet also considering its country specific needs and requirements.[30]

3.1.2 Key legal regimes

Australia has yet to pass any direct legislation in relation to quantum preparedness, although, as discussed in more detail below, a range of quantum technologies have been regulated for decades in Australia through export controls[31]. Preparedness in Australia can be found in part in the SOCI Act, which operates as an 'all hazards' risk management framework for critical infrastructure industries and contains flexible and adaptive mechanisms to absorb quantum-related risks. Direct legal obligations relevant to quantum technology relate to export controls under the Defence and Strategic Goods List 2024 and

---

[23] Australian Government, 'Cyber Security Strategy' (n 13).
[24] Ibid 33.
[25] Australian Government '2023-2030 Australian Cyber Security Strategy Action Plan' *(Plan)* https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf 13.
[26] Australian Government, *Information Security Manual (ISM)* (Web Page) https://architecture.digital.gov.au/information-security-manual-ism accessed 25 April 2024. See also the NIST standardization process: https://csrc.nist.gov/projects/post-quantum-cryptography accessed 21 August 2024.
[27] See Appendix E for details.
[28] See Regulatory Horizons Council, 'Regulating Quantum Technology Applications' (Report, February 2024) https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf.
[29] Regulatory Horizons Council, 'Regulating Quantum Technology Applications' (Report, February 2024) https://assets.publishing.service.gov.uk/media/65ddc83bcf7eb10015f57f9f/RHC_regulation_of_quantum_technology_applications.pdf. 6
[30] Australian Government, 'Cyber Security Strategy' (n 13).
[31] For example, 'quantum cryptography' has been listed on the Defence and Strategic Goods list 2024 (DSGL) since 1996.

foreign investment restrictions in critical technology industries. The Defence and Strategic Goods List 2024 (DSGL) (a legislative instrument authorised under the *Customs Act 1901* (Cth))[32] specifies goods, software and technology that are 'controlled' items under Australian export control legislation. A permit is required when exporting, supplying, brokering or publishing DSGL items, unless exempted. Part 2 of the DSGL lists 'dual-use' goods which are developed for commercial purposes but could also be used for military purposes. These 'dual use goods' include quantum crytography, quantum key distribution, post-quantum, quantum-safe or quantum-resistant algorithms and quantum computers[33]. However, these controls are severely diluted or removed when the technology is in the 'public domain'.[34]

It is worthwhile noting that export restrictions can be a double-edged sword. A key principle of cryptosystem design argues against a 'security by obscurity' approach. Instead, proponents of this design principle argue that exposure of the system design to the public may be helpful in the following ways:

(1) assuming attackers will know the system in detail means that your design and key security will be stronger; and

(2) broad 'peer review' of the system can assist in uncovering previously unknown flaws and weaknesses.[35]

Quantum technologies, including quantum cryptography, quantum computers and quantum communications, are listed on Australia's *List of Critical Technologies in the National Interest*.[36] The list interacts with the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA). The *Foreign Investment Reform (Protecting Australia's National Security) Act 2020* (Cth) amended the FATA so that definitions associated with critical technology, and critical infrastructure in SOCI are now included in the FATA. Foreign investment in a responsible entity or a direct interest in a critical infrastructure asset is now subject to notification to the FIRB. FIRB can undertake 'own motion' review of transactions if it has national security concerns.[37]

See Appendix A for more detail on Australia's regulation, policy and strategy.

3.1.3 Implications of quantum technology for Australia's extant national security frameworks - examples

The following obligations may be incompatible with communications and data storage and processing industry efforts to secure their communication channels with strong cryptographic systems designed to protect against interception and access.[38] On the one hand, regulated entities are required to 'do their best' to secure their assets from unauthorised access and take an 'all-hazards' approach to risk management. On the other hand, there is an expectation that certain critical infrastructure industry participants –

---

[32] S 112(2A)(aa).
[33] DSGL 3.E, 4.A.901, 5.A.2.
[34] DSGL ss 3.94, 3.101(2), 3.111, Category 5 Parts 1 and 2.
[35] Eric Diehl, *Ten Laws for Security* (Springer International Publishing AG, 2016) <http://ebookcentral.proquest.com/lib/unsw/detail.action?docID=4744597>. Ch 3.
[36] Department of Industry, Science and Resources, 'List of Critical Technologies in the National Interest', Australian Government (Web Page, 19 May 2023) < https://www.industry.gov.au/publications/list-critical-technologies-national-interest>.
[37]For more details, see FIRB Foreign Investment Review Board, *Guidance Note* 8 - *National Security Test* (Guide, 17 December 2020) < https://firb.gov.au/sites/firb.gov.au/files/guidance-notes/G08-Nationalsecurity.pdf>.
[38] For a discussion of the issues and possible solutions, Carnegie Endowment for International Peace, *Moving the Encryption Policy Conversation Forward* (Working Group Report, 10 September 2019) https://carnegieendowment.org/2019/09/10/moving-%20encryption-%20policy-%20conversation-forward-pub-79573.

telecommunications and data storage and processing - will also provide access and assistance to their services, systems, and networks.

The SOCI Act[39] imposes Federal cyber security and other obligations on designated critical infrastructure (CI) industries responsible for declared CI assets. In this context, CI assets are assets considered 'essential to the functioning of the economy, society, or national security' of Australia.[40] The SOCI Act established a register of CI assets and has economy-wide coverage of regulated industries including electricity, gas, water, and maritime port sectors. It applies to data storage or processing, communications, financial services, and energy, as well as many other sectors. The SOCI Act contains extensive statutory obligations relating to CI assets,[41] including:

- obligations on the operator to:
  - notify the Australian Signals Directorate (ASD) of any cyber incidents impacting CI assets;[42] and
  - establish, maintain, and comply with an all-hazards critical infrastructure risk management program (CIRMP);[43] and
- the ability of the government to:
  - in the case of some cyber-attacks, require the responsible entity to provide information, take or refrain from taking action, and/or authorise the ASD to intervene to defend the asset;[44] and
  - declare certain CI assets as 'Systems of National Significance' ('SoNS'), subjecting the responsible entity to enhanced cyber security obligations, such as incident response plans, cyber security exercises, government access to system information and mandatory cyber security exercises.[45]

A recent consultation paper on proposed legislative reforms in the wake of the new Cyber Security Strategy[46] did not contain any quantum-specific reforms, although it is likely that quantum attacks would be subject to some of the SOCI Act provisions, particularly under an 'all-hazards' CIRMP. The consultation paper sought views on a legislative reform proposal to incorporate the telecommunications sector security regulatory framework with the SOCI Act. This reform would harmonise the telecommunications sector's security with that of other critical infrastructure industries, including aligning telecommunications within the 'all-hazards' risk management framework.[47]

---

[39] *Security Legislation Amendment (Critical Infrastructure) Act 2021*; *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth).
[40] Gilbert + Tobin, 'A Guide to Critical Infrastructure Assets in Australia' (*Web Page*, 2022) www.gtlaw.com.au/knowledge/guide-critical-infrastructure-assets-australia. The definition of 'CI assets' in s 9 of *Security of Critical Infrastructure Act 2018* (Cth) does not define this term generally, but by reference to industry assets.
[41] The asset definitions are set out in *SOCI Act* s 12F and the *Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021* (Cth) ('CIRMP Rules').
[42] *SOCI Act* pt 2B.
[43] *SOCI Act* pt 2A.
[44] *SOCI Act* pt 2B.
[45] *SOCI Act* pts 6A and 2C.
[46] Australian Government, *2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper*, (Issued 8 Jan 2024) https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/cyber-security-legislative-reforms.
[47] Ibid.

Australian law enforcement and intelligence agencies possess powers to obtain access to encrypted communications.[48] Under Part 14 of the TA, carriers and certain carriage service providers must, among other things, give authorities 'such help as is reasonably necessary' for the purposes of enforcing criminal laws and laws imposing pecuniary penalties; protecting public revenue; and safeguarding national security. In addition, carriers, carriage service providers and carriage service intermediaries must 'do their best' to protect telecommunications networks and facilities from unauthorised interference or unauthorised access, including, for the purposes of security, protecting the confidentiality of communications and the availability and integrity of telecommunications networks and services.

Part 15 of the TA authorises a range of technical assistance that security and law enforcement agencies may request from designated communications providers (although noting the type of assistance is constrained by the specified function of the requesting Agency). For example, in the case of the Australian Signals Directorate, giving assistance may include providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored, or communicated by electronic or similar means. Authorised assistance may include removing electronic protections and facilitating access to a range of services, devices, and software.

Carriers and carriage service providers also have obligations under Part 5-3 of the TIA to provide interception capability of their telecommunications systems, permitting interception of communications and delivery of the intercepted communications.

Quantum information technologies will impact the national security obligations of critical infrastructure sectors as those technologies evolve and are commercially deployed. For example, a future regulated operator or provider of a quantum communications system or network marketed to customers as a 'premium secure service' may not be technically able to provide interception capability, unless that capability is part of the network or system design. Likewise, "interception-by-design" in a secure quantum communications network or system may be neither economically desirable nor technically feasible due to the quantum mechanics operating the system or network. Equally, a fault tolerant quantum computer may be both friend and foe in an interception scenario, providing both offensive and defensive capability to governments or industry participants.

The quandaries posed by quantum information technologies that we have identified in this brief require careful consideration by government, including further research and co-designed solutions with critical infrastructure industry participants.

3.2 Overview of EU law and policy

The EU has announced significant ambitions in developing quantum technologies. However, it has also publicly recognised the risk posed to current cryptography practices.[49] On 11 April 2024, the European Commission released a recommendation that member states commence developing strategies for a coordinated response and eventual adoption of post-quantum cryptography.[50]

---

[48] *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), which amended the TA, the TIA, the *Surveillance Devices Act 2004* (Cth) and various other related legislation.
[49] See Appendix B.
[50] European Commission, 'Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography', Policy and Legislation (Web Page, 11 April 2024) https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography.

3.2.1 Key legislation

There is no quantum-specific preparedness legislation in place in the EU related to cyber security. However, on 18 April 2023, the European Commission proposed the Cyber Solidarity Act,[51] an EU Regulation to improve the preparedness, detection and response to cyber security incidents across the EU. The proposal includes a European Cybersecurity Shield to protect, detect, defend and deter cyber threats, including post-quantum encryption.[52] Additionally, in April 2024 the European Commission issued a formal Recommendation that 'Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible'[53] and proposed the Member States collaborate to produce a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' and evaluate and select PQC algorithms as EU standards.[54]

Regulation (EU) 2021/821[55] sets out rules throughout the EU to control exports, brokering, technical assistance, transit and transfer of 'dual-use' items. Controlled items include quantum computers and related electronic assemblies and components, qubit devices and qubit circuits containing or supporting arrays of physical qubits, quantum control components and quantum measurement devices; as well as the technology for their development or production.[56]

3.2.2 Quantum standards development

In general, European standards are created by one or more of the following standards organisations: CEN, CENELEC or ETSI. The CEN-CENELEC Focus Group on Quantum Technologies released a standardisation roadmap for the EU in March 2023.[57] In 2021, ETSI released two Technical Reports (TRs) to support the US National Institute of Standards and Technology (NIST) standards for quantum cryptography. To date, ETSI has published several Technical Reports, Technical Specifications and Group Reports on quantum technologies, primarily on quantum-safe cryptography, VPNs and signatures.[58]

See Appendix B for more detail on EU regulation, policy and strategy.

---

[51] Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents Proposal 2023 (EU) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209.

[52] European Commission, 'A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton', *Speech* (Web Page, 05 April 2023) https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145.

[53] European Commission, 'Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography' https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography Recital 5.

[54] Ibid, cl 1.

[55] *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)* [2021] OJ L 206 11.6.2021/1.

[56] Ibid art 9(4).

[57] CEN-CENELEC Focus Group on Quantum Technologies (FGQT) *Standardization Roadmap on Quantum Technologies* (Release 1 – March 2023) https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf.

[58] ETSI, *Search and Browse Standards* (Web page) https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-12-19&harmonized=0&keyword=&TB=856,,836&stdType=&frequency=&mandate=&collection=&sort=1.

3.3 Overview of Indian law and policy

In January 2024, the Indian Ministry of Electronics and Information Technology released its Quantum Technologies Roadmap for consultation, prioritising research and development in 'thrust areas', such as cyber security.[59] India announced its first 'quantum secure communication link' in March 2023, between the Department of Telecommunications and the National Informatics Centre.[60] In April 2023, it announced funding of in excess of INR6000 crore (USD 730 million) for quantum projects under its National Quantum Mission.[61] By October 2023, India had nearly a hundred quantum projects in development.[62] It has also entered into several public, private and university partnerships. However, this funding and these projects are not confined to cyber security and encryption issues: rather, their scope is broad and includes computing, communications, sensing and metrology, and materials and devices.[63]

3.3.1 Key legislation

India has several ministerial divisions with some responsibilities for overseeing the development of quantum technology. However, it is yet to put into effect preparedness regulatory or legal frameworks specific to quantum technology. It is currently proposed that a new Digital India Act (DIA) will replace the existing *Information Technology Act 2000*. The DIA is expected to contain provisions attempting to address the risks of emerging technologies, including strengthened cyber security obligations.[64]

Like many other countries, India regulates quantum technologies through export controls. *The Foreign Trade (Development & Regulation) Act* 1992 (India) regulates India's international trade. The Directorate General of Foreign Trade (DGFT) publishes the Foreign Trade Policy (FTP), which governs exports and imports of goods and services. Under the FTP 2023, 'export of dual-use items, including software and technologies, having potential civilian/industrial applications as well as use in weapons of mass destruction is regulated. It is either prohibited or is permitted under an authorization.'[65] Dual-use items are listed in the Special Chemicals, Organisms, Materials, Equipment and Technologies list (SCOMET), and includes: quantum cryptography, quantum key distribution (QKD), superconducting quantum interference devices, as well as many cryptographic and cryptanalytic technologies.

India's foreign direct investment (FDI) is governed by the *Foreign Exchange Management Act 1999* (FEMA). The current FDI Policy has been effective since 2020 and does not include guidelines on quantum technology. Existing rules for the Information Technology sector allow for 100% FDI. However, eleven sectors require government approval for FDI, including

---

[59] Ministry of Electronics and Information Technology, 'Quantum Technologies Roadmap', Government of India (Web page, 23 January 2024) https://www.meity.gov.in/content/project-timeline-qc-roadmap-v5.
[60] 'India's First Quantum Computing-Based Telecom Network Link Now Operational: Ashwini Vaishnaw', *The Economic Times* (online, 27 March 2023) https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99026697.cms ('India's First Quantum Computing-Based Telecom Network Link Now Operational').
[61] 'Cabinet Approves National Quantum Mission to Scale-up Scientific & Industrial R&D for Quantum Technologies', *PMIndia* (19 April 2023) https:/www.pmindia.gov.in/en/news_updates/cabinet-approves-national-quantum-mission-to-scale-up-scientific-industrial-rd-for-quantum-technologies.
[62] Ministry of Science & Technology, 'Industry will be expected to be a major resource contributor in all the future StartUp ventures and other new technology initiatives, says Union Minister Dr Jitendra Singh' (*Press Release*, 5 October 2023) https://pib.gov.in/PressReleseDetailm.aspx?PRID=1964650.
[63] See Appendix C.
[64] Ministry of Electronics and Information Technology, 'Proposed Digital India Act 2023', *Digital India Dialogues* (9 March 2023) <https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf>.
[65] Directorate General of Foreign Trade, 'Chapter 10: Special Chemicals, Organisms, Materials, Equipment and Technologies'. *Foreign Trade Policy 2023* https://content.dgft.gov.in/Website/dgftprod/a2f58730-df83-49df-a437-b5f6345abb66/FTP2023_Chapter10.pdf.

some sectors likely to involve quantum technologies (eg mining, defence, satellites, telecommunications, some financial services and pharmaceuticals).[66]

3.3.2 Quantum standards development

The Bureau of Indian Standards (BIS) is the national standards body of India. Its Electronics and IT Division Council (LITDC)[67] is primarily responsible for developing Indian standards in the field of electronics and IT products and has a technical committee for quantum computing.[68] BIS's objectives include aligning Indian standards with international ones.[69]

See Appendix C for more detail on India's quantum regulation, policy and strategy.

3.4 Overview of UK law and policy

The UK has made significant investments as part of its National Quantum Technologies Programme 2014-2024 (NQTP) and National Quantum Strategy 2023-2033 (NQS) (public and private funding of GBP 1 billion in the NQTP, and a planned GBP 3.5 billion in the NQS).

3.4.1 Key legislation

The NQS is cognisant of the risk that advanced quantum computing poses to much of existing public-key cryptography. The National Cyber Security Centre (NCSC UK) has stated that existing quantum computers cannot do this, but the current threat is rather the interception and stockpiling of encrypted data *now*, with an intention to decrypt in the future once quantum computing has developed that capability. The NCSC UK has issued guidance on the use of quantum key distribution (QKD) and 'quantum-safe cryptography' (QSC).[70] The guidance states that QKD is not suitable for military or government applications due to hardware requirements, and the use of *non-standardised* QSC is not recommended.[71]

The *Regulation of Investigatory Powers Act 2000* (UK) (RIPA) and the *Investigatory Powers Act 2016* (UK) (IPA) together comprise the main regime for interception of communications by UK public authorities. IPA allows for interception and acquisition of communications data, and RIPA governs the obtaining of electronic data protected by encryption. There is no specific mention of quantum technologies.

The *National Security Investment Act 2021* (UK) (NSIA) allows the UK government to scrutinise and intervene in certain acquisitions made by anyone, including businesses and investors, that could harm the UK's national security. Notification is required in 17 sensitive areas of the economy, *including* quantum technologies (as well as several other sectors likely to use quantum technologies, such as communications, computing hardware, and advanced materials.)[72]

---

[66] Foreign Investment Facilitation Portal, 'Present FIFP', (Web Page) https://fifp.gov.in/AboutUs.aspx.
[67] Electronics and IT Division, Bureau of Indian Standards, 'Strategic Roadmap', (Web Page) https://www.services.bis.gov.in/tmp/ELECTRONICS%20AND%20IT%20DIVISION%20COUNCIL.pdf.
[68] Bureau of Indian Standards, 'LITD C : P5 - Quantum Computing Panel', (Web Page) https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/dgdashboard/committee_sso/composition/604/4.
[69] Bureau of Indian Standards, 'Standards National Action Plan (SNAP) 2022-27', https://www.bis.gov.in/wp-content/uploads/2023/05/SNPbookBilingual.pdf 55.
[70] National Cyber Security Centre (UK), 'Preparing for Quantum-Safe Cryptography' (*Whitepaper*, 11 Nov 2020), https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.
[71] It is possible that the UK will encourage QSC based on standards developed by either NIST or ETSI, when these are complete.
[72] Cabinet Office (UK), 'National Security and Investment Act: details of the 17 types of notifiable acquisitions' (*Guidance*, 6 Feb 2024) https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions

The UK's Export Control Order 2008, which regulates the export of dual-use goods also applies to some quantum technologies.[73] In March 2024, the UK amended the Export Control Order 2008 to include quantum computers, qubit devices and qubit circuits, quantum control components and quantum measurement devices and computers, including "electronic assemblies" and components containing certain integrated circuits.[74]

The UK has recently signalled that it will introduce the Cyber Security and Resilience Bill in 2025.[75] The bill aims to improve cyber security and resilience in critical infrastructure sectors in the UK due to the increasing prevalence and sophistication of emerging technologically mediated threats. The bill will uplift the existing NIS Regulations 2018. Quantum computers and cryptography have been noted as a future threat by the NCSC UK.[76]

See Appendix D for detailed information on the UK's quantum policy and regulation.

3.4.2 Quantum standards development

The UK has recently (Nov 2023) established the Quantum Standards Network Pilot,[77] which appears to be focused on encouraging UK involvement in international standards systems rather than UK-specific standards. The UK National Cyber Security Centre (NCSC) has indicated that it is waiting on the NIST and ETSI post-quantum standards. The UK is also engaging in conversations on technical standards for quantum with organisations such as the IEEE Standards Association, IOS and IEC.[78]

3.5 Overview of US law and policy

The US has implemented a legislative framework (focusing heavily on government agencies) in anticipation of the widespread availability of quantum computing, cryptography and communications. Policy is clearly driven by national security concerns as well as the economic benefits to be derived from quantum commercialisation.

3.5.1 Key legislation

In 2018, the Trump government established the National Quantum Initiative (NQS) under the *National Quantum Initiative Act 2018*, which concentrated on funding the research activities of NIST, the National Science Foundation and the Department of Energy. Funding for quantum activities has also been made available under the *National Defense Authorisation Act (2019, 2020, 2022)* (NDAA) for defence activities and the *CHIPS and Science Act 2022* for semiconductor chips that can be used in quantum communications.

The US is attentive to the risks of quantum computing acting upon conventional encryption practices. On 21 December 2022 the *Quantum Computing Cybersecurity Preparedness Act 2022*[79] (QCCPA) became law in the US. Section 4 of the QCCPA puts into effect a multi-phase scheme guided by the Office of Management and Budget (OMB) to require federal agencies to (1) inventory and report any IT that is vulnerable to decryption by quantum computers; and

---

[73] From 1 April 2024, the export of '[q]uantum computers and components, as well as software and technology for the development or production of quantum computing' will be subject to the issuing of an export licence under the Export Control (Amendment) Regulations 2024 (UK).
[74] See Export Control (Amendment) Regulations 2024 (UK)
[75] Department of Science, Innovation and Technology, Cyber and Resilience Bill, 30 September 2024 https://www.gov.uk/government/ collections/cyber-security-and-resilience-bill
[76] Felicity Oswald, CYBERUK2024: Keynote Address (Speech 14 May 2024) https://www.ncsc.gov.uk/speech/cyberuk-2024-ncsc-ceo keynote-speech
[77] National Physical Laboratory (NPL), *Quantum Standards Network Pilot*, https://www.npl.co.uk/quantum-programme/standards/network-pilot, accessed 25 April 2024.
[78] Department for Science, Innovation and Technology, *National Quantum Strategy* (Mar 2023) https://www.gov.uk/government/publications/national-quantum-strategy#:~:text=A%2010%2Dyear%20vision%20and,the%20UK's%20prosperity%20and%20security ('NQS'). 30
[79] H.R. 7535, main operative provisions 6 USC 1526.

(2) when NIST post-quantum cryptography (PQC) standards are issued, develop a plan to migrate their IT to PQC. While national security systems are exempt from the QCCPA (s5), requirements to migrate these systems to PQC standards are covered under an earlier executive order.[80] The NDAA also authorised the Department of Defense to 'increase the technology readiness level of quantum information science technologies under development in the United States, support the development of a quantum information science and technology workforce, and enhance awareness of quantum information science and technology'.[81]

There are various state and federal communications electronic surveillance laws. One important example is the *Communications Assistance for Law Enforcement Act 1994* (CALEA). CALEA required telecommunications carriers to assist law enforcement in intercepting electronic communications where a court order exists. However, providers cannot generally be required to build in access points or decrypt data. The requirements now apply to some broadband and VoIP providers due to administrative action from the Federal Communications Commission. The Foreign Intelligence Surveillance Act 1978 and the PATRIOT Act have also been used to mandate the cooperation of phone companies in collecting connection metadata.[82] However, it is worth noting that US law enforcement has not been very successful in decryption of intercepted encrypted content: eg in 2019, law enforcement could not decrypt 438 out of 464 instances of interception encrypted communications.[83]

The Export Control Reform Act 2018 regulates the export of emerging and 'foundational' dual use technologies including some quantum technologies. In September 2024, the US Commerce Department's Bureau of Industry and Security (BIS) issued an interim final rule (IFR) on export controls for quantum computing (along with semiconductor and additive manufacturing items).[84] The IFR established a new licensing arrangement that enables countries with equivalent controls to export technologies without submitting a licence application, subject to conditions. The UK and Australia enacted similar controls for quantum technologies in 2024.

3.5.2 Quantum standards development

The US appears to primarily rely on national standards developed by its own standards body, the National Institute of Standards and Technology (NIST).[85] The most significant standard released by NIST to date relates to three draft quantum resistant cryptographic algorithms released in August 2023. NIST approved three Federal Information Processing Standards

---

[80] Joseph Biden Jr, 'Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems' *National Security Memorandum/NSM-8* (4 May 2022) https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[81] National Quantum Coordination Office, 'About the National Quantum Initiative' <*quantum|gov*> (Web Page) https://www.quantum.gov/about/

[82] Scott F Mann, 'Fact Sheet: Section 215 of the USA PATRIOT Act' (*Commentary*, Center for Strategic & International Studies, 27 Feb 2014) https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act

[83] https://crsreports.congress.gov/product/pdf/IF/IF11769

[84] Bureau of Industry and Security, 'Department of Commerce Implements Controls on Quantum Computing and Other Advanced Technologies Alongside International Partners' (Media Release, 5 September 2024) < https://www.bis.gov/press-release/department commerce-implements-controls-quantum-computing-and-other-advanced>.

[85] See National Institute of Standards and Technology, Post-Quantum Cryptography Standardisation (Web Page) https://csrc.nist.gov/pqc-standardization. On 13 August 2024. NIST finalised its 'principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer.' NIST advised that 'the algorithms are specified in the first completed standards for NIST's post-quantum cryptography standardisation project.' (Media Release) https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized- post-quantum-encryption-standards.

(FIPS) for post-quantum cryptography in August 2024.[86] It is expected that the algorithms will withstand a future cyber attack by a quantum computer. The National Security Agency released quantum algorithm requirements for national security systems in 2022.

See Appendix E for detailed information on the UK's quantum policy and regulation.

3.6 International standards

On 11 January 2024, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) announced the establishment of a joint technical committee (JTC 3) on quantum technologies, whose professed scope is to 'develop standards in the field of quantum technologies, and more particularly quantum computing, quantum simulation, quantum sources, quantum metrology, quantum detectors and quantum communications'.[87] The IEC/ISO JTC3 – Quantum Technologies committee is due to meet in October 2024.[88] The ISO/IEC has already published a two-part standard relating to quantum key distribution requirements, evaluation and testing.[89] The IEEE Standards Association has also several quantum standards projects currently in development, including projects on post-quantum network security, post-quantum cryptography migration, and quantum computing.[90]

3.7 Summary of regulatory frameworks

Country	Import/Export of Dual Use Goods	Foreign Investment Rules	Quantum 'Preparedness' Legislation
Australia	✓	✓	✗
United States	✓	✓	✓
European Union	✓	✓	✗
United Kingdom	✓	✓	✗
India	✓	✓	✗

[86] NIST, "Announcing approval of the Federal Information Processing Standard (FIPS) for post-quantum cryptography.' (Media Release 13 August 2024)
[87] ISO, 'IEC and ISO launch new joint technical committee on quantum technologies' (*News*, 11 Jan 2024) https://www.iso.org/news/new-joint-committee-quantum-technologies
[88] International Electrotechnical Commission, JTC3/23A/DA – Revised Draft Agenda for the meeting of the IEC/ISO/JTC 3 to be held in Edinburgh, United Kingdom on 21-22 October 2024
[89] Eg ISO/IEC 23837-1:2023 (Requirements) and ISO/IEC 23837-2:2023 (Part 2: Evaluation and testing methods).
[90] IEEE SA (Standards Association) 'Quantum Standards and Activities' (*Web Page*) https://standards.ieee.org/practices/foundational/quantum-standards-activities/ accessed 25 April 2024

4 Conclusion

Quantum information technology applications present significant challenges to cybersecurity worldwide, with the potential to compromise encrypted systems. This policy brief focuses on Australia's preparedness in the face of evolving quantum technology applications. The brief recommends the following actions for Australian governments:

- **Recommendation 1: Design adaptable quantum resilient regulation for the short, medium, and long term.**

  The United States has the most advanced regulatory approach to quantum information technology among the countries reviewed. An examination of both procedural and substantive legal and regulatory tools, including mapping extant regulatory frameworks and determining whether they are operationally 'fit for purpose' in the face of quantum threats, would be a good place to begin the design process for adaptable, resilient regulation.

- **Recommendation 2: Incorporate quantum standards into existing frameworks**.

  Standards will be crucial as the quantum information technology ecosystem evolves over time. Australia is already involved at the highest levels in quantum standardisation. The mapping exercise in Recommendation 1 should be extended to standards to identify which frameworks are operationally 'fit-for-purpose' to adopt quantum standards as they are developed and adopted.

- **Recommendation 3: Contribute more funding for Australian quantum-resilient development.**

  Resilience is a governance and regulatory concept that can be applied in the context of emerging technologies to design strategies, substantive and procedural measures and overarching governance frameworks. Commencing research and development around the concept of quantum resilience would assist in the development of an adaptive approach. Researchers, developers, innovators, civil society, critical infrastructure industries and governments should be encouraged to contribute to this work through workshops, roundtables and in co-design networks, such as the TISN.

- **Recommendation 4: Continue to advocate for standards development.**

  Australia is already at the forefront of quantum standards development through the strategic initiatives and involvement of Australia's quantum researchers, the Department of Industry, Science and Resources, Standards Australia and the CSIRO. Researchers, developers, innovators and governments should continue to be encouraged to contribute to this important work through workshops, roundtables and co-design networks.

- **Recommendation 5: Explore security and law enforcement capabilities.**

  The resilience of security and law enforcement capabilities to quantum information technologies will become a pivotal operational concern as quantum computing, communications and cryptography are deployed with uncertain impact and effect. We recommend a comprehensive, independent, expert exploration and inventory of security and law enforcement capabilities vis-à-vis the challenges and opportunities of quantum

information technologies. This study should include impact on relevant national security law and policy frameworks, in addition to the forecasted impact of the technology itself. This study should seek to identify both substantive and procedural issues and concerns and make recommendations.

- **Recommendation 6: Develop the Australian Public Service into a quantum workforce**.

  The Australian Public Service needs to be trained, maintained and retained as a 'quantum-ready workforce'. This upskilling should include targeted recruitment of candidates with subject matter knowledge and expertise, training for current APS members, including targeted training for operational and policy teams. Lessons from the deployment of AI and other emerging technologies should be incorporated into a feasibility or skills study of the APS, including an initial survey of knowledge and expertise in new and emerging technologies, and recommendations. Research should also explore options for driving collaboration and knowledge exchange about quantum resilience in the APS, including secondments, bespoke training courses, scenario testing and tabletop exercises.

- **Recommendation 7: Contribute to better understanding of the impact of quantum computing on other emerging technologies and associated risks.**

  Australia is well placed to contribute to the understanding of the impact of quantum computing on other emerging technologies and their associated benefits and risks. Increasing domestic and international research collaboration with a multi-factorial, inter-disciplinary approach should be encouraged and funded, so that the interplay between various elements of the emergence of quantum technologies can be studied and policy responses developed and adapted.

- **Recommendation 8: Promote collaboration and partnerships between public, private and research sectors to enable development and utilisation of tools for easier access and testing.**

  In the quantum field, Australia has a strong track-record of successful collaboration and partnerships between the public, private and research sectors. What is needed now are a range of tools and mechanisms to test and utilise technologies and provide access to potential users and customers of the technology. We have seen joint-ventures, co-investment and sharing of complex resources already in the quantum ecosystem. But we recommend further funding, research and supportive policies to encourage interoperability, common standards and collaborative testing and improvement.

- **Recommendation 9: Establish resilient quantum supply chain following a risk-based approach.**

  Establishing a resilient quantum supply chain using a risk-based approach will be essential for future deployment of quantum technologies in the Australian economy. Current work being done on supply chain resilience should be expanded to include quantum technologies. For example, the Office of Supply Chain Resilience within the Department of Industry, Science and Resources could be well placed to undertake this work by partnering with researchers, other government departments and agencies and industry participants to identify critical supply chain vulnerabilities in the quantum supply chain. Further research could also focus on the supply chain resilience framework and its efficacy and effectiveness for quantum technologies.

- **Recommendation 10: Develop guidelines for users and vendors of quantum computing solutions (e.g., hardware requirements and impact on performance).**

  There are challenges and benefits in developing guidelines for users and vendors of quantum computing solutions. Australia is well placed to develop robust guidelines that support safe and effective development and use of quantum computing solutions. There are successfully operating examples that provide a blueprint for such work. For example, the Australian Signals Directorate has had success with its Essential 8 Maturity Model guidelines for a graduated cyber security posture. In 2022-2023, ASD completed numerous Cyber Maturity Measurement Program assessments for federal, state and territory entities, and performed Cyber Security Uplift services. Private and public organisations can access the Essential 8.

In conclusion, the brief recognises the need for an adaptive approach to address the evolving challenges posed by quantum advancements. It serves as a foundation for further research and policy development.

5 Appendices