Appendix E USA Quantum Policy and Regulation[1, 2]

Currency date 1 September 2024

Table of Contents

1. Legislation Summary 2
2. What has the USA done to date on Quantum strategy, policy and legislation? 2
3. How is the USA approaching quantum technology in strategy and policy? 3
4. Does the USA have quantum specific legislation? If so, what does it cover? What does it do? 3
5. What technologies are mentioned in the USA's quantum strategy and policy? 5
6. What competition/competing interests are mentioned/raised/ identified in the USA's quantum strategy and policy? 5
7. Is there consideration of the impact of quantum computing and quantum communications? 5
8. Does the USA's approach to quantum consider/mention quantum-safe encryption, quantum cryptography? 6
9. What does the USA's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption? 6
10. Does the USA's approach to quantum mention any specific regulatory or legal frameworks? If so, which frameworks? If so, what is the predicted impact of quantum on those frameworks? If so, does the approach outline any possible solutions? 6
11. Are there any international or national standards identified in the USA's approach to quantum technology? If so, what are they and where do they come from? 6
12. Does the USA's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected? 7
13. Does the USA's approach to quantum technology discuss critical technology and dual- use regulatory and legal frameworks? 7
14. Are there any gaps identified in the USA's approach to quantum technology? Are there any barriers and challenges identified in the USA's approach? Are there any advantages to the USA's approach? 7
15. Has the USA strategy mentioned other countries? 8
16. Does the USA's strategy consider critical infrastructure and supporting technologies? eg cryogenics (for QC cooling) 8
17. Legislation 9
18. Coordinating Bodies 9
19. Agencies 10

[1] Prepared by Catherine Nguyen with contributions from Jennifer Westmorland, UNSW Allens Hub for Technology, Law and Innovation.

[2] Appended to Lloyd-Jones, Susanne and Kayleen Manwaring, 'Quantum Resilience in the Australian National Security Legislative Framework' (Policy Brief, Cyber Security Cooperative Research Centre, UNSW Faculty of Law & Justice, September 2024)

1. Legislation Summary

The USA has passed several pieces of legislation dealing with different aspects of their quantum mission. The first piece of legislation directly related to quantum was the **National Quantum Initiative Act** (NQI Act) passed in 2018. The NQI Act was passed to enable the NIST, DOE and NSF to develop and operate programs related to QIS in the US. These programs have included the establishment of research centres, institutes, and a National Quantum Initiative Advisory Committee.

Each year since the passing of the NQI Act, the **National Defense Authorization Act** (NDA Acts FY 2019, 2020 and 2022) which specifies the annual budget for the Department of Defense (DOD), have legislated QIS related activities. Examples from the 2022 NDA Act include a grant program for QIS education in the Junior Reserve Officers' Training Corps and activities to 'accelerate the development and deployment of dual-use quantum capabilities'.

The **CHIPS and Science Act 2022** was passed to provide $280 billion in funding for semiconductor chips and makes mention of quantum networking and communications applications of chips.

The **Export Control Reform Act 2018** deals with emerging and 'foundational' dual use technologies which include quantum technologies, however, the NDA Acts will likely be more informative on dual-use quantum technologies.

The **Quantum Computing Cybersecurity Preparedness Act 2022** required federal agencies to maintain an inventory of information technology in use by the agency that is vulnerable to decryption by quantum computers within 6 months of the Act. It then requires federal agencies to develop a plan to migrate their systems to post-quantum cryptography within 1 year of NIST issuing their post-quantum cryptography standards.

Potential legal frameworks for quantum include:

Communications Assistance for law Enforcement Act 1994 (CALEA) is a wiretapping law that enhances the ability of law enforcement agencies to conduct lawful interception of communication by requiring telecoms to modify their equipment to have targeted surveillance capabilities.

The **Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Bill** and **Lawful Access to Encrypted Data Bill** attempted to restrict E2EE and could have impacts on quantum.

2. What has the USA done to date on Quantum strategy, policy and legislation?

The USA's quantum policy started with the National Quantum Initiative Act (2018) enacted by the Trump Administration. The National Quantum Initiative is a whole-of-government approach to ensuring American leadership in QIS, their strategy is outlined in a number of strategy documents including:

- National Strategic Overview for Quantum Information Science 2018
    - first strategy document – six areas of policy: science, workforce, industry, infrastructure, economic security, and international cooperation.
- Bringing Quantum Sensors to Fruition 2022
- A Coordinated Approach to Quantum Networking 2021
- Quantum Frontiers 2020
- A Strategic Vision for America's Quantum Networks 2020
- National Security Memorandum on Quantum-Resistant Cryptography 2022
- The Role of International Talent in Quantum Information Science Report 2021
- QIST Workforce Development National Strategic Plan 2022

These published strategies have been assisted by legislation (see Q4) and presidential directives/memos to action the formation of QIS committees, roundtables, research centres and QIS programs.

3. How is the USA approaching quantum technology in strategy and policy?

The USA are focussed on being the global leaders in quantum technology. The quantum.gov website states that 'the National Quantum Initiative is a whole-of-government approach to ensuring American leadership in QIS'. (see further in Q15)

Their strategy for R&D and related activities is set out in the 'National Strategic Overview for QIS'[1]. The Strategic Overview states that the strategy focusses on: 'getting the science right', 'enhancing competitiveness', and 'enabling people'.

The USA seem to have established a top-down government approach to quantum technology. Compared to Australia, their strategy documents make little mention of specific private companies in the quantum space rather, they pinpoint plans for pre-existing federal agencies. The key piece of legislation regarding quantum serves to COORDINATE existing federal bodies NIST, NSF and DOE.

4. Does the USA have quantum specific legislation? If so, what does it cover? What does it do?

The USA has both quantum specific legislation and quantum-related legislation.

- **Quantum – specific**:

National Quantum Initiative Act (2018): established the National Quantum Initiative; accelerated quantum research and development by authorizing new activities, programs, and centers at NIST, NSF and the DOE. The Act expired in September 2023.

Post-Quantum Cybersecurity Standards Act[3]**: t**his bill was introduced in September 2023. The purpose is to amend the National Quantum Initiative Act and the Cyber Security Research and Development Act to advance the rapid deployment of post quantum cybersecurity standards across the United States economy and support United States cryptography research. The Director of NIST, in consultation with the Secretary of Homeland Security and the heads of sector risk management agencies, is to promote the voluntary adoption and deployment of post-quantum cryptography standards. These efforts will be supported by the granting of funds, dissemination of publicly available guidance and resources. Technical assistance will be provided to entities that are at high risk of quantum cryptoanalytic attacks.

Quantum Instrumentation for Science and Engineering Act[4]**:** This Bill was introduced to the House of Representatives in October 2023. The purpose is to amend the National Quantum Initiative Act in order to accelerate quantum research and development in the United States. It directs the NSF to award grants to upgrade and support research and development in quantum information science, technology, and engineering. This bill will also enable better access to resources, materials, devices and the critical services needed to enable cutting-edge research on quantum information science, as well as to train the next generation of quantum scientists and workers. It will also support the translation of research into commercial products and services.

National Quantum Initiative Reauthorisation Act[5]**;** the bill was introduced November 2023, to reauthorise the expired National Quantum Initiative Act. Requires the White House Office of Science and Technology Policy to develop a strategy for carrying out cooperative

[3] https://www.congress.gov/bill/118th-congress/house-bill/5759/history?s=1&r=18
[4] https://www.congress.gov/bill/118th-congress/house-bill/5950/text?s=1&r=34
[5] https://www.congress.gov/bill/118th-congress/house-bill/6213

quantum research efforts with allies of the United States to bolster competitiveness against China and Russia. Directs the Secretary of Energy to develop a strategy for promoting the commercialization of quantum computing. Facilitates interagency partnerships to advance quantum technology. Authorizes the DOE to support the development of resources to meet the needs of the quantum supply chain. Requires the creation of a Quantum Institute at NASA. Authorizes NIST to establish centres to advance research in quantum sensing, measurement, and engineering. Strengthens educational and workforce programs at NSF.

The Support For Quantum Supply Chains Act[6]: introduced to the House of Representatives in November 2023. This bill will amend the National Quantum Initiative Act to accelerate the development of supply chain supporting technology for quantum information science, technology, and engineering; support United States competitiveness and reduce risks in the quantum supply chain.

Expanding Capacity in Quantum Information Science, Engineering, and Technology Act, or the "Expand QISET Act"[7]: this bill was introduced in November 2023. It is designed to increase research capacity, education, infrastructure capacity and participation in quantum information science, engineering, and technology and related disciplines. It directs the National Science Foundation (NSF) to make awards and grants that support curriculum development and to fund quantum education pilot programs. The NSF is tasked with securing a talent pipeline to meet the quantum workforce needs of industry, government, and academia.

Defence Quantum Acceleration Act of 2024[8]: this bill was introduced in April 2024. The primary purpose is to direct the Secretary of Defense to accelerate the implementation of quantum information science technologies within the DoD, including the development of prototypes. This is landmark legislation in that it specifically requires quantum technology to become an integral part of USA Defence capabilities. It authorises the establishment of a multi-disciplinary QIS Centre of excellence. It also establishes a new Quantum Advisor role in the DoD, who will coordinate with the armed forces commands on the use and challenges of quantum technology within the DoD, as well as with industry, academics and allies such as AUKUS and NATO.

- **Quantum – related:**

Cyber Security Research and Development Act (2002):[9] authorizes appropriations to the National Science Foundation and to the National Institute of Standards and Technology to establish new programs, and to increase funding for computer and network security research and development, including research fellowships.

Export Control Reform Act (2018): regulates the export of emerging and 'foundational' dual use technologies which includes some QT but NDAA will be more relevant.

National Defense Authorization Act (FY 2019, 2020): authorises DOD to increase technology readiness level of QIS tech, authorisation to coordinate all QIS and technology R&D within the DOD. The FY 2024 Act requires the Pentagon to establish a pilot program on near-term quantum computing applications[10].

[6] https://www.govtrack.us/congress/bills/118/hr6207/text
[7] https://www.congress.gov/bill/118th-congress/house-bill/6384/text?s=1&r=31
[8] https://www.congress.gov/bill/118th-congress/senate-bill/4105/text
[9] https://www.congress.gov/bill/107th-congress/house-bill/3394#:~:text=Cyber%20Security%20Research%20and%20Development%20Act%20%2D%20Authorizes%20appropriations%20to%20the,programs%2C%20for%20computer%20and%20network
[10] https://www.govinfo.gov/content/pkg/CRPT-118hrpt125/pdf/CRPT-118hrpt125.pdf

CHIPS and Science Act (2022): amended NQIA to authorise R&D in quantum networking infrastructure development of standards in quantum networking and communication, integration of QIS and engineering into STEM curriculum for all.

Quantum Computing Cybersecurity Preparedness Act (2022): Requires agencies to establish an inventory of information technology that is vulnerable to decryption by quantum computers. Later requires agencies to develop a plan to adopt NIST post quantum cryptography standards.

The Department of Defense Appropriations Act 2024[11]**:** provides FY2024 appropriations to the Department of Defense for military activities and includes multiple budget increases for quantum technology programs.

5. What technologies are mentioned in the USA's quantum strategy and policy?

The USA generally groups the quantum technologies into the following 3 or 4 categories: quantum **sensing**, quantum **communications**, quantum **simulations**, quantum **computing**. (quantum simulation and quantum computing are sometimes combined).[2]

Quantum Sensing

- Atomic clocks
- Atom interferometers
- Optical magnetometers
- Devices utilising quantum optical effects
- Atomic electric field sensors

Quantum Communications

- Quantum networks`

Quantum Computing/Simulations

- Quantum cryptography

6. What competition/competing interests are mentioned/raised/ identified in the USA's quantum strategy and policy?

Innovation v security is the main debate in the USA's strategy and policy. The USA's goal is to lead the world in the quantum industry, and this would necessarily mean that policy should not stifle innovation and competition. China is frequently mentioned as a key competitor to USA's leadership in quantum. (see Q15 for more on international competition). However, quantum technology has been identified as dual use technology that can have military use and therefore needs to be subject to regulation. This competition of interests can be seen in the enactment of the Export Control Reform Act 2018 (see Q13).

7. Is there consideration of the impact of quantum computing and quantum communications?

The impact of quantum computing and communications is mainly discussed in relation to national security interests.

> The nation that harnesses quantum communications technology first may be able to decode — in a matter of seconds — every other nations' most sensitive encrypted national security information as well as proprietary technologies and even the personal information of individuals.[12]

[11] https://www.congress.gov/bill/118th-congress/house-bill/4365

[12] John Thune, 'U.S. must win the race against China and Europe on quantum computing', John Thune U.S. Senator for South Dakota (*Opinion Editorial*, 26 July 2018) < https://www.thune.senate.gov/public/index.cfm/op-eds?ID=B5B2BC8E-8551-4731-A52D-7B583199F782>.

8. Does the USA's approach to quantum consider/mention quantum-safe encryption, quantum cryptography?

Yes, see Q9 for further.

The Department of Homeland Security issued a policy directive in 2021 about preparing for post-quantum cryptography. It states that

> DHS has significant national security concerns across mission spaces including critical infrastructure, law enforcement, privacy, and counterintelligence that could be harmed by insufficient preparation for a transition to post-quantum cryptography.[3]

9. What does the USA's approach to quantum technology say about current encryption practices and processes? Does it mention that quantum will 'break' current encryption?

The USA has made it clear that their current encryption standards are vulnerable quantum computing cryptography breaking.

> Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC (cryptographically relevant quantum computer[13]

Their strategies make it a priority to mitigate the risk by transiting to quantum resistant cryptography which will be released by NIST (see Q11).

10. Does the USA's approach to quantum mention any specific regulatory or legal frameworks? If so, which frameworks? If so, what is the predicted impact of quantum on those frameworks? If so, does the approach outline any possible solutions?

US academia has flagged the following legislation as possible regulatory frameworks for quantum:

Communications Assistance for law Enforcement Act (CALEA)

- purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance

Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Bill

- Attempted to outlaw strong encryption/E2EE
- Failed to pass in 2020, reintroduced in 2022, and for a third time in 2023.

Lawful Access to Encrypted Data Bill

- Introduced to congress but seems to have stalled ~ 2020

This bill requires certain technology companies to ensure that they can decode encrypted information on their services and products in order to provide such information to law enforcement. It also establishes requirements and procedures for assisting law enforcement agencies in accessing encrypted data.

11. Are there any international or national standards identified in the USA's approach to quantum technology? If so, what are they and where do they come from?

From their strategy documents, the USA seems to primarily rely on national standards developed by its own standards body, the National Institute of Standards and Technology (NIST). The most significant standard released by NIST thus far of three draft quantum-

[13] White House, 'National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems' (*Memorandum*, 4 May 2022).

resistant cryptographic algorithms. The draft was publicly released in August 2023 and NIST is seeking feedback until November 2023. They are expected to release the formal standard in 2024. Additionally, some current standards applying to true random number generators (eg NIST SP 800-90B and NIST-800-22) can be used to assess quantum random number generators.[14]

The National Security Agency has released quantum algorithm requirements for national security systems in 2022.

The USA does not seem to mention the implementation of international standards such as those developed by the IEEE Standards Association.

12. Does the USA's approach to quantum technology discuss barriers or challenges of quantum technology? If so, what are they? What will be affected?

The main challenge of quantum *cryptography* is the transition to the new algorithms, which includes:

- Replacement of algorithms requires changing or replacing cryptographic libraries, implementation validation tools, hardware changes, dependent operating system, and application code communication devices, protocols and user and administrative procedures.
- Security standards, procedures, and best practice documentation need to be changed or replaced, as do installation, configuration, and administration documentation.

The challenges of adopting and using post-quantum algorithms is explored in the NIST White Paper titled 'Getting Ready for Post-Quantum Cryptography'[15]

More generally, the US Quantum Strategy 2018 Paper identified 4 key challenges:

1. Coordinating government action with the public and private institutions
2. Requiring a broad and viable workforce to enact R&D
3. Strong interdisciplinary connections
4. Maintaining strong industrial engagement

The above challenges will need be addressed to maintain and expand American leadership in QIS technology.

13. Does the USA's approach to quantum technology discuss critical technology and dual-use regulatory and legal frameworks?

Critical Technology (refer to Q16 for critical infrastructure)

Dual Use Regulation and Frameworks

- There is brief mention of the Export Control Reform Act 2018 deals with emerging and 'foundational' dual use technologies which include quantum technologies.

14. Are there any gaps identified in the USA's approach to quantum technology? Are there any barriers and challenges identified in the USA's approach? Are there any advantages to the USA's approach?

The DHS Secretary stated that much of the US's critical infrastructure is in the private sector's hands and says that the DHS should work with the private sector to protect

[14] Leilei Huang et al, 'Quantum Random Number Cloud Platform' (2021) 7(1) *npj Quantum Information* 1.

[15] Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms – NIST – 28 April 2021

American interests. I think there may be a gap in USA's strategy in their more limited recognition of the private sector. As discussed earlier, the US strategy focusses heavily on their existing federal agencies and there is less emphasis on the private sector. There is also less discussion of commercialisation of QIS tech compared to Australia's strategy.

15. Has the USA strategy mentioned other countries?

The USA seem to be most worried about Chinese progress on quantum technologies. Security concerns are usually cited as the reason for this worry. China has stated that one of its main goals is to surpass the USA in the quantum field.
'In testimony before Congress, expert witnesses have warned that as other nations around the world rapidly advance their own quantum programs, the U.S. faces a real threat of falling behind.'[16]

16. Does the USA's strategy consider critical infrastructure and supporting technologies? eg cryogenics (for QC cooling)

The USA's strategy recognises that QIS R&D will rely on the availabilities of tools, facilities, and infrastructure and that these will be sourced from supporting industries. The strategy recommends expansion of Federal and industrial infrastructure and support activities to accelerate progress in the QIS field.

> Agencies will be encouraged to explore mechanisms to provide the QIS research community with increased access to existing and future Federal facilities, including manufacturing facilities that can be repurposed and expanded as well as systems and testbeds for post-quantum applications.[17]

[16] John Thune, 'U.S. must win the race against China and Europe on quantum computing', John Thune U.S. Senator for South Dakota (Opinion Editorial, 26 July 2018) < https://www.thune.senate.gov/public/index.cfm/op-eds?ID=B5B2BC8E-8551-4731-A52D-7B583199F782>.
[17] Subcommittee On Quantum Information Science, *National Strategic Overview For Quantum Information Science* (Report, September 2018).

17. Legislation

NQIA	National Quantum Initiative Act 2018	Authorises research activities for NIST, NSF, and DOE
NDDA	National Defense Authorization Act	Authorises DOD to increase technology readiness level of QIS tech, authorisation to coordinate all QIS and technology R&D within the DOD.
CHIPS-Plus	CHIPS (Creating Helpful Incentives to Produce Semiconductors) and Science Act 2022	Authorises $110 billion for basic and advanced technology research over 5 years (including quantum computing)

18. Coordinating Bodies

SCQIS	Subcommittee on Quantum Information Science	The National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science (SCQIS) coordinates Federal research and development (R&D) in quantum information science and related technologies under the auspices of the NSTC Committee on Science. The aim of this R&D coordination is to maintain and expand U.S. leadership in quantum information science and its applications over the next decade. The SCQIS is co-chaired by the Office of Science and Technology Policy (OSTP), the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF) and the Department of Energy (DOE).
ESIX	NSTC Subcommittee on Economic and Security Implications of Quantum Science	The National Science and Technology Council (NSTC) Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) was established to ensure that economic and security implications of QIS are understood across the agencies. The subcommittee provides a national security perspective to QIS related research. The ESIX Subcommittee coordinates with NSTC subcommittees, such as the SCQIS, to ensure that the economic and national security implications of basic research and development in QIS, along with derived technologies are fully understood. The subcommittee is co-chaired by the Office of Science and Technology Policy (OSTP), Department of Defense (DOD), Department of Energy (DOE), and the National Security Agency (NSA).
NQCO	National Quantum Coordination Office	The National Quantum Coordination Office (NQCO) is legislated by the NQI Act to carry out the daily activities needed for coordinating and supporting

		the NQI. The Coordination Office is tasked with providing technical and administrative support to the SCQIS, ESIX and the NQIAC as well as overseeing the interagency coordination of the NQI Program. The NQCO serves as the primary point of contact on Federal civilian quantum information science and technology activities and conducts public outreach, including the dissemination of findings and recommendations of the SCIQS and the Advisory Committee, as appropriate. The NQCO staff are federal employees on detail assignments from across the government.
NQIAC	National Quantum Initiative Advisory Committee	The National Quantum Initiative Advisory Committee (NQIAC) is the Federal Advisory Committee called for in the NQI Act. The NQIAC is tasked to provide an independent assessment of the NQI Program and to make recommendations for the President, Congress, and the NSTC Subcommittee on QIS to consider when reviewing and revising the NQI Program. The NQIAC consists of leaders in the field from industry, academia, and the Federal laboratories. The NQIAC was first established by Executive Order 13885 on August 30, 2019. It was subsequently enhanced by Executive Order 14073 on May 4, 2022.

19. Agencies

NIST	The National Institute of Standards and Technology	Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic prosperity. As authorized by the NQI Act, NIST is coordinating consortia focusing on quantum technologies, and maintaining fundamental QIS R&D programs. NIST has been a leader in QIS R&D for over three decades., including a seminal workshop on QIS at its Gaithersburg campus in 1994.
DOE	The Department of Energy	Ensures America's prosperity and security through several mechanisms including basic and applied scientific research, discovery and development of new technologies, and scientific innovation. The Energy Department's National Laboratories are a system of intellectual assets unique among world scientific institutions and serve as regional engines of economic growth for states and communities across the country. As authorized by the NQI Act,

		DOE is strengthening core programs and establishing new Centres focusing on QIS research.
NASA	The National Aeronautics and Space Administration	Drives advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality and stewardship of Earth. NASA's research portfolio includes some activities focusing on, and motivated by, quantum information science.
DOD	The Department of Defense	Engages in basic research, defined as the 'systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind.' DOD has supported fundamental QIS research for three decades, and continues to invest in basic QIS R&D activities via several DOD offices, agencies, and laboratories. These include: the Office of the Under Secretary of Defense for Research and Engineering (OUSDRE); the Defense Advanced Projects Agency (DARPA); the Army Research Laboratory (ARL), the Army Research Office (ARO); the Naval Research Laboratory (NRL); the Office of Naval Research (ONR), the Air Force Research Laboratory (AFRL); and the Air Force Office of Sponsored Research (AFOSR).
LPS	Laboratory for Physical Science	University, industry, and federal government scientists collaborate on research in advanced communication, sensing, and computer technologies, the LPS currently houses four main divisions related to information science and technology, including Solid-State and Quantum Physics.
IARPA	The Intelligence Advanced Projects Activity	Sponsors several applied research programs that explore quantum computing.
NSF	National Science Foundation	The National Science Foundation is an independent agency of the United States federal government that supports fundamental research and education in all the non-medical fields of science and engineering. NSF co-chairs the SCQIS.