The Post-Quantum Cryptography Migration Starts Today

Version 1.0

TABLE OF CONTENTS

Introduction

This paper has been developed by the Digital Government Exchange (DGX) cyber security working group and input from subject matter expert organisations. Please refer to the Acknowledgements section for further details.

It will be presented at the 2024 DGX Conference in September to ensure that a consensus-based proposed approach for migrating to Post-Quantum Cryptography (PQC) is robust and widely supported.

The paper is intended for policy, technology, and financial leaders involved in securing government networks and protecting critical infrastructure.

The Threat of Quantum Computing to Government Cryptography

Cryptography and digital signatures are essential to keeping government secrets confidential and maintaining the functionality of the internet. They prevent nefarious actors from masquerading as legitimate users and accessing or seizing control of sensitive systems. These schemes are nearing a breaking point. Public and private sector systems will be at risk once a quantum computer of sufficient size and sophistication is deployed. Due to their unique position safeguarding national and economic security, **governments must act now to protect their cryptographic systems**.

Since the 1980s, scientists have theorised about the advent of a machine that applies quantum physics to computing. Recent innovations have turned this idea into a reality as primitive quantum computers exist today. Once quantum computers reach scientific maturation, they are expected to break commonly used cryptography that powers internet confidentiality and authentication, meaning that **much of the public-key cryptography used today will be broken once a quantum computer is deployed**.

There is a substantial impact to national and economic security if cryptographic systems can be undermined by a future quantum computer. Breaking cryptography means adversaries could commit wide-scale financial fraud, interrupt critical infrastructure services, and access the most classified and sensitive state secrets. Beyond the future impact of a quantum computer, **there is a threat to systems today**. While quantum computers have not reached scientific maturity to threaten cryptography, **adversarial actors have the resources for intercepting and gathering encrypted data today to decrypt it once they have a quantum computer**. This is particularly relevant for governments, as certain information remains sensitive for decades. Its disclosure may threaten national secrets and future operational capacity.

The threat of quantum computers is here, and attackers are using this avenue to their advantage. Nations are actively investing in quantum computing research and development. An adversarial nation could use quantum computers to target government information, allowing them to jump significantly ahead in their intelligence collection and give them an unrivalled, strategic advantage. This has the potential to create a national security threat.

This presents a hard problem for government, compounded by additional challenges that underscore the urgency to begin work to mitigate the threat today.[1] It is not known when strong enough quantum computers of sufficient scale will be deployed, as advancements create a level of uncertainty around this timeline. The complex operating environment adds to this challenge as governments are likely unaware of their level of vulnerability due to third-party providers and the ubiquitous nature of cryptography. Government legacy systems are not designed to be easily updated, which can complicate transitions to post-quantum cryptography.

Furthering these challenges, protecting cryptography requires substantial government investment. The system upgrades required due to Y2K cost the U.S. Government around $15 billion in today’s money, and cost the world up to $900 billion. The scale of funding necessitates sustained commitment and creates additional obstacles to securing government systems. While the threat of quantum computers presents a difficult challenge to governments, **there is a solution and leaders can act now to secure their systems**.

[1] Please see Annex B for an explanation of the challenges that complicate the cryptography transition.

The Solution to the Quantum Threat

There is a solution to mitigate the threat of quantum computers to government systems. Since 2016, governments, academia, and industry have been working on cryptography that cannot be broken by a quantum computer. These cryptographic algorithms are based on different mathematical problems that do not have the vulnerabilities of today's algorithms. The National Institute of Standards and Technology (NIST) spearheaded this **global competition to solicit, evaluate, and finalise PQC algorithms**. After assessing 82 algorithms from 25 countries, three were standardised and released on 13 August 2024.

The specific algorithms that governments select depend on individual technical requirements and policies. All governments must consider two things before selecting an algorithm. First, it is vital that governments implement algorithms that have gone through robust testing processes so that a vulnerability is not discovered after wide-scale deployment. Second, these algorithms must also be interoperable and perform well with existing communications protocols and networks to reduce the need to replace systems entirely.

Once governments select their algorithms, they will use these to replace vulnerable cryptography. The solution to the quantum threat entails a cryptographic transition, which is not an easy task. Previous transitions took decades, and the post-quantum algorithms have unique technical aspects that make them complicated to implement.

Given the profound implications for national security and economic stability, and the challenges associated with migrating to PQC algorithms, **it is imperative for government to begin the post-quantum transition today**. Governments can begin work, or build off existing initiatives, through four high-level steps:

1. Asset Management: Conduct an inventory of cryptographic algorithms across government systems and identify priority areas for migration. Since governments are not aware of their threat level until an inventory is completed, this work should begin right away. Robust inventories ensure leaders are aware of vulnerable cryptography throughout their supply chain and what systems need to be prioritised.
2. Lifecycle Management: Allocate sufficient funding to ensure a successful overhaul of government cryptography. The transition to PQC will require substantial resources. Governments can work with their budgeting authority now to ensure officials are aware of the threat and start planning the needed future funding.
3. Change Management: Upgrade their cryptographic infrastructure to support quantum-resistant algorithms. Once governments have inventoried their systems, allocated funding, and ensured the algorithms they select have undergone rigorous testing, the transition can begin. This means swapping out current cryptographic algorithms and implementing agile systems to enable future transitions at lower cost.
4. Vulnerability Management: Regularly audit their systems for vulnerabilities and ensure future resilience. The final step of the transition process is promoting continuous security of government cryptographic systems. The new algorithms are not a silver bullet. Governments need to maintain resilience through active monitoring of their systems for security weaknesses and enabling crypto-agility.

The most important step for governments is to act now. The greatest resource at our disposal is time, and if we start the work to transition systems today, we can mitigate the quantum threat.

Acknowledgements

The development of this paper was led by the DGX UK and U.S. members in close collaboration with the DGX cyber security working group and subject matter expert organisations including UK NCSC, NIST, BSI, CCCS, and NL NCSC.

Special thanks to the following DGX cyber security working group members for their content contributions and insights. Their cooperation and willingness to share information have been crucial to the development of the content.

- Donald Ong, Senior Consultant, Cloud Cyber security Programme Office, Singapore
- Martin Bowyer, Deputy Director for Security, Central Digital and Data Office, United Kingdom
- Philip Stupak, Assistant National Cyber Director, Office of the National Cyber Director, The White House, United States
- Po Tea-Duncan, Chief Information Security Officer of the Government of Canada, Office of the Chief Information Officer,Treasury Board of Canada Secretariat, Canada
- Stephan Ehlen, Cryptography Expert, German Federal Office for Information Security (BSI), Germany
- Tuija Kuusisto, Senior Ministerial Advisor, Public Sector ICT, Ministry of Finance, Finland
- Andrew Morrison, Chief Technology Officer, Digital Transformation Agency, Australia
- Lesly Goh, World Bank Senior Technology Advisor & Singapore GovTech Board Member

References

1. Next steps in Preparing for Post-Quantum Cryptography | UK NCSC
2. Transitioning to a Quantum-Secure Economy | World Economic Forum
3. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House
4. Quantum-Readiness: Migration to Post-Quantum Cryptography | CISA
5. Getting Ready for PQC: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms (CSWP 15) | NIST
6. Projects – Post-Quantum Cryptography | NIST
7. Quantum-Safe Cryptography – Fundamentals, Current Developments and Recommendations | BSI
8. Report on Post-Quantum Cryptography | The White House
9. Addressing the Quantum Computing Threat to Cryptography (ITSE.00.017) | CCCS
10. The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography | NL National Communications Security Agency
11. 2023-2030 Australian National Cyber Security Strategy | Department of Home Affairs

Annex A: The Weight of the Quantum Threat

When it becomes available, a [quantum computer] could jeopardise civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions. – U.S. National Security Memorandum 10

Quantum computing solves certain mathematical problems significantly faster than classic computing systems. This ability introduces a threat to cryptographic algorithms used to protect data and verify the authenticity and integrity of messages. Most public-key cryptography algorithms in use today rely on the security of a function which is easy to compute in one direction (e.g., multiplying prime numbers) and incredibly difficult to compute in the other (e.g., factorising large numbers). A quantum computer of sufficient sophistication is projected to be able to compute these problems exponentially faster due to Shor’s algorithm, potentially compromising much of the traditional public-key cryptography used today.

There is a **substantial impact to national and economic security if current public-key cryptography can be broken by a quantum computer**. The security of nearly all internet communications today relies on public-key cryptography as it protects the confidentiality and integrity of data. First, cryptography protects the confidentiality of data since it underpins current encryption systems. Encryption is used to ensure messages sent over the internet are not readable to any other user besides the recipient. Cryptography also validates the integrity of communications. Digital signatures use public-key cryptography and are vital for email authentication, phishing and spoofing prevention, software update validation, payment security, and fraud protection. Websites use certificates based on public-key cryptography to validate the website’s identity. Breaking public-key means an attacker could fake official government communications, causing vast misinformation and operational disruptions.

Critical infrastructure, such as military communications and technology that delivers vital services to its citizens, relies on cryptography that keeps data secure and authenticates commands on its control systems. **Breaking cryptography could disrupt the delivery of critical infrastructure services** run by the government, such as energy grids, healthcare systems, and transportation networks.

If a government were communicating about sensitive information, a quantum computer could access this sensitive information. Imagine a government is working on a highly classified blueprint for a defence innovation – something that if their adversaries knew about, could radically weaken their military strength. Without the confidentiality provided by encryption, this information could be exposed and cost the country billions, if not trillions, in investment. Adversaries could also discover critical weaknesses in defensive systems. This is especially relevant to the quantum computing threat, as these large military innovations often remain in circulation for decades. **If a malicious actor can collect this blueprint information today, a country’s warfighting capability of tomorrow is jeopardised**. The extent of the national and economic security threat underscores the urgency to begin the work to transition government systems today.

Annex B: Government Challenges to Adopting PQC

The quantum threat to cryptography is compounded by several challenges for governments that underscore the urgency to transition systems today. First, significant technological breakthroughs in recent years make it **hard to predict the timescales for a cryptographically-relevant quantum computer (CRQC) to materialise.** Some leading experts in the field forecast the quantum threat could materialise in as soon as 10 years.[2] This uncertainty may encourage leaders to postpone action. However, any delay in transitioning to PQC could result in inadequate preparation and increased risk when quantum computing becomes capable of breaking current cryptography.

Another complication with the post-quantum transition is that **cryptography is highly prevalent throughout systems**. Governments are likely to be unaware of where they have cryptography that is vulnerable to a quantum computer. This means governments do not know their current level of risk. Additionally, government organisations manage very high-value classified data. This data could be a target for harvesting, where adversaries collect encrypted data today with the intent to decrypt the data in the future using quantum computers. Governments have to not only be aware of where they are vulnerable, but also what assets are the highest priority to secure today.

Next, government tends to heavily rely on **suppliers and technology vendors** who operate government infrastructure and critical services. This reliance often comes with limited visibility into the full supply chain, creating dependencies that can complicate efforts to minimise quantum threats. The prevalence of public technology tools in government systems that are maintained by single developers, such as open-source software, compounds this issue. This lack of transparency and control makes it challenging to ensure that all components of the supply chain are quantum-resistant, increasing the risk of exploitation using quantum computing capabilities.

Also, the government carries a significant amount of **legacy information technology** — outdated technology and software — which are rarely updated to mitigate known vulnerabilities. This is often due to compatibility issues or the complexity of the system. Over time, these systems accumulate security weaknesses that can be exploited by adversaries. The lack of updates makes them more vulnerable to quantum computing attacks that can easily break outdated cryptographic protections. Some of these systems can have cryptographic algorithms hardwired, requiring a more intensive update of the technology. It is important to note that PQC upgrades can be rolled into general cyber security upgrades, allowing both of these accumulated security weaknesses to be solved at the same time.

Finally, the **distributed structure of governments** can also add additional challenges to the transition. For example, in decentralised agency structures, the lower-level authorities are often not regulated to collect information about government-wide cryptography. Since the agencies operate independently, they can decide how much information to disclose throughout the government. The decentralised nature of certain governments also means that awareness of the quantum threat can be quite low, especially among regional or local authorities. These entities may not be willing to participate in the inventory or allocate funding to the transition. Addressing this must be done in parallel to the inventory effort.

[2] Michele Mosca and Marco Piani, 2023 Quantum Threat Timeline Report, Global Risk Institute, December 2023, https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/.

Annex C: Conduct an Inventory of Relevant Systems

Before you migrate to PQC, it is important to make an inventory of your data to be protected, its confidentiality period and the cryptography you use. – The Netherlands General Intelligence and Security Service.

Governments should begin by spearheading an inventory of their systems to better understand their level of risk and how they can prioritise transition efforts. An appropriate government inventory would survey all systems, applications, and devices to catalogue the cryptographic algorithms in use and should span all environments, including on-premises, cloud, and hybrid setups. It is **important to engage with supply chain vendors to identify technologies that rely on quantum-vulnerable cryptography** and ensure that third-party products and services are also transitioning to PQC.

The inventory can be a lengthy, resource-intensive process, but there are opportunities to make this easier. Depending on an organisation's third-party reliance, governments can have vendors conduct inventories of their provided systems. There is also an **opportunity to automate the inventory process** using advanced technology solutions. Making the inventory easier is an area where international collaboration is key – sharing lessons learned will make the process more efficient for all governments.

This inventory is important to identifying which systems governments should prioritise with transition resources. Linking algorithms to the specific information they protect and the required duration of that protection will help in prioritising which systems need immediate attention. Inventories help understand where governments have high impact systems, and how long it will take to upgrade systems based on their unique technical requirements.

Prioritisation should be given to high impact systems, industrial control systems, and systems with long-term confidentiality needs. Specifically, highly sensitive information that needs to be protected for decades is at greater risk as adversaries could use the harvest now, decrypt later approach. Comparatively, information that loses its value quickly may not be at risk of such attacks, and can therefore be considered later in the priority list if it does not support a high value function.

In addition to identifying high value systems that protect vital information, **an inventory helps discover how much time it will take to upgrade or update a system**. Since there are a variety of systems in government, each individual one must be technically analysed to better understand its transition timeline. For example, a lengthy hardware upgrade may need to be prioritised over an easier software one. Once governments have an understanding of the vulnerable cryptographic algorithms in their systems and the type of infrastructure it supports, they can better prioritise system transitions. This inventory can also assist with government efforts on crypto-agility and preparing for future threats to cryptography.

Lastly, it must also be recognised that **the government's inventory must be protected**; the same data that governments need to guide migration to PQC could be used as a roadmap for bad actors. Adversaries may be seeking to gain a strategic advantage using quantum computers, and the exposure of a government's vulnerabilities and priority systems would make this process much easier for them. Governments should be sure to secure these inventories with strong cyber security practices to prevent their exposure.

Annex C-1: The U.S. Process for Cryptographic Inventory

The United States' PQC transition began in 2022, with President Biden's *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. This directive outlines initial steps for the government to begin the transition, including an inventory of cryptographic systems within federal agencies, and a preliminary cost estimate for migrating systems to PQC. Agency inventories provide government leaders at all levels insight into vulnerabilities of current cryptographic systems, while cost estimates provide understanding of the scale of the work needed to migrate existing systems.

This case study identifies lessons learned from the U.S. inventory experience so far and provides a potential framework for future governments to replicate when embarking on their PQC transition. A detailed description of the U.S. inventory process can be found in the memorandum on *Migrating to PQC* released by the Office of Management and Budget in 2022, and the *Report on Post Quantum Cryptography*, released in 2024.

U.S. agencies have been asked to address questions in four major areas.

First, agencies need to understand **what systems they have and their relative value and importance**. Many countries already have this information categorised, distinguishing high value assets and providing other identifiers to establish cyber security standards appropriate to the system. This also allows information security professionals to understand the system in the larger agency and government context.

Second, for each system, they need to identify **what cryptographic techniques are being used**. This provides awareness of the scope of vulnerable cryptography within agency systems, while also allowing the identification of overlapping migration requirements that could impact the transition process.

Third, it is important for agencies to **understand the source of each government system**. In particular, the high prevalence of systems provided by commercial developers has implications for migrating cryptographic systems. While vendors may be motivated to upgrade cryptographic algorithms due to other commercial pressures, government procurement policy may need to evolve to accurately reflect the need for post-quantum cryptographic systems.

Finally, governments need to be aware of **any existing plans that affect the PQC transition**. The planned deprecation, replacement, and refresh of government systems provide opportunities to incorporate PQC into existing plans, simplifying the migration.

The unique agency structures of each nation, and their individual technical requirements, may result in an inventory process that looks significantly different from country to country. However, in starting the migration process, the U.S. has learned some key lessons. In particular, by carrying out an inventory of cryptographic systems, the scope of the problem has become clear. **Migrating systems will take time and resources, and with the impending threat of quantum computers, governments should begin the process now**. While work will vary between nations, this case study articulates that the inventory is a manageable process if governments are methodical about their actions and prioritise effective planning.

Annex D: Allocate Sufficient Funding

Dedicating the appropriate amount of resources to support the transition is vitally important to ensuring its success. Alongside its inventory of government systems, the U.S. has directed departments and agencies to prepare an estimate of how much they believe the transition will cost. The U.S. experience revealed funding requirements will fall into two major categories: technology and people. First is the price of actually transitioning the algorithms, including the hardware, software, and facilities expenses. Second is the personnel needed to implement upgrades, which can often be more than the technology itself. It is important for governments to prepare for the “people” cost, in addition to the technological upgrades.

The U.S. cost estimate also revealed the inventory process can assist with cost requirements. One of the reasons why it is important to understand the future plans for government systems is because **PQC can be incorporated into technology refurbishment**. This can enable the migration to PQC while implementing cyclical updates to systems, potentially reducing costs and streamlining efforts. Additionally, thoughtful use of vendors for government services can ease the burden to update cryptographic methods if the company plans to update their cryptography.

Countries have unique budgetary structures, including restrictions on single-year funding and decentralised structures, that can complicate the funding needed for a successful transition. Governments can drive coherence for public organisations to ensure funding matches the quantum threat. The U.S. and Canada created processes to **align budget requests with high-level cyber security goals** through the *Administration Cybersecurity Priorities* and *Enterprise Cybersecurity Strategy*. Both of these documents mention the need to prioritise resources for the PQC transition. The goal is to use these documents to require government divisions to incorporate the post-quantum transition in their annual budgets and ensure long-term continuity in prioritising these system upgrades.

It would be helpful for many governments to know a high-level cost number to complete the PQC transition, but this is difficult to proactively determine. In the U.S., since inventory efforts are ongoing, this cost estimate has a high degree of uncertainty. While accurate numbers are not available, **governments can look at the cost estimate for historical examples of system overhauls due to substantial risk**, such as the Y2K bug. Prior to the turn of the century, many were concerned that the changing of the date from 1999 to 2000 would render many technology systems inoperable. To remedy this issue, it is estimated the U.S. government spent around $8.5 billion, with total U.S. investment including the private sector being $100 billion (€91 billion, £77 billion, S$132 billion). This is over $180 billion (€163 billion, £140 billion, S$237 billion) today. Estimates for the rest of the world were up to $500 billion, or $912 billion today (€830 billion, £709 billion, S$1.2 trillion). [3]

The 2000 threat of systems being inoperable presented a substantial national security and economic risk, similar to the threat faced by quantum computers. With this level of risk comes a high price tag for protection. The Y2K numbers demonstrate **system upgrades can be an expensive task and underscore the need to begin cost conversations with government leaders today**

[3] “Y2K Aftermath – Crisis Averted,” The United States Senate Special Committee on the Year 2000 Technology Problem, February 29, 2000, https://permanent.access.gpo.gov/lps90964/y2kfinalreport.pdf.

Annex D-1: International Support for Developing Countries

The most urgent near-term threat for [low- and middle-income countries] from quantum technologies is the development of cryptographically capable quantum computers…. However, a timely transition to those protocols requires technical capabilities that [low- and middle-income countries] governments often lack. – U.S. Agency for International Development (USAID)

The quantum threat is a global problem. With the interconnected nature of our digital communications, the world's collective resilience is only as strong as the weakest point in the supply chain. This means it is vital to support a range of countries with the PQC transition. It is especially important to ensure developing countries are provided the tools to successfully mitigate the threat and transition with the rest of the world.

Developing countries often have limited resources allocated for information technology modernization and infrastructure upgrades. High-profile cyber-attacks on developing countries in recent years exemplify the capacity gap and how these countries remain targets for malicious actors. Many of the systems are fragmented and outdated, with frequently unpatched software and antiquated hardware. These countries lack the qualified technology expertise about PQC to properly assess the magnitude of the problem and take actions for mitigation.

Developing countries could especially benefit from international collaboration to tackle the threat of quantum computers. This collaboration could help raise the awareness of the vulnerability and provide the needed resources for the transition, including capacity building for policymakers and their information technology staff. Awareness of the threat is the first step for achieving buy-in, and it is important for more developed countries to help communicate the issue to these countries' leadership. Once countries are aware of the threat and understand the risk of not taking action, the work to protect systems can begin.

Past understanding the problem, **international collaboration can help these countries develop the needed resources for a successful transition**. Resources include financial backing to upgrade current algorithms and sharing lessons learned from countries further along in the process. This backing could come from bilateral or multilateral agreements, philanthropic funding, or development projects from state agencies. Sharing lessons learned can ease the burden for developing countries so they do not make the same mistakes as ones who have already completed this work and would help guide them in the right direction. All of these solutions help increase capacity, something that will be key to convincing leadership this should be a priority and the country can successfully make this transition.

There is also the need to recognize international collaboration and investment can help **advance the general cyber security posture of these countries**. Enabling strong cryptographic protocols is a core cyber security issue and ensures that the entire system is built on security. This would not just be an investment in one technical solution, but rather would increase the ability for these countries to protect themselves against traditional cyber security threats in addition to quantum computers. Work to support developing countries can start now. If a few developing countries take the first step to address the PQC challenge, it will inspire the others to follow.

Annex E: Transition Cryptographic Algorithms

[PQC] seems like a simple solution to the threat from a potentially disruptive technology. And conceptually, it is - but the migration to PQC is a very complicated undertaking. – UK National Cyber Security Centre (NCSC)

Once there are adequate resources to support the cryptography transition, governments should begin the work of upgrading their systems. This entails a robust process – **governments must select the right algorithms and dedicate time for the transition.**

The security of these algorithms is paramount to a successful transition. Since 2016, NIST has led a global competition to develop, evaluate, and standardise PQC. These algorithms have undergone substantial development and testing to ensure protection against a quantum computer. Out of 82 algorithms submitted, three were standardised on 13 August 2024. It is vital that governments implement algorithms that have gone through significant testing that was open, public, and transparent, so that a vulnerability is not discovered after deployment.

Security is important for all algorithms, but the **algorithm selected for a specific government system will depend on the requirements of its infrastructure**. Technical differences between the algorithms mean some might work better for certain government systems than others. One algorithm might be easier to implement based on the hardware or software of the system, another might require less compute resources. Governments must analyse the performance and interoperability of the algorithms with its unique systems. And governments should select algorithms that have undergone public scrutiny.

Previous cryptographic transitions demonstrate that **migrating systems is not an easy task**. There are still systems in the U.S. that have not completely finished the last cryptographic transition that started 20 years ago. This demonstrates that transitions take substantial time, especially from government stakeholders, and leaders should ensure time is given to implement the new standards. Furthering the time challenge, the algorithms have varying technical requirements, such as different key lengths and processing times. This will make their implementation more lengthy than previous transitions. The time needed also presents an opportunity, especially for developing countries that have not transitioned to modern cryptographic algorithms. These systems that have still not been updated can transition straight to PQC, bypassing the previous update.

The deployment process will be intensive, but governments can ease this burden by **prioritising the high-value systems** identified in the inventory. These are the systems where their exposure or failure would have consequential impacts on national and economic security. Within government systems, there are moderate or low value assets that do not hold the same impact. Since many countries have timelines to upgrade and replace legacy technology, these systems can hopefully be secured with traditional lifecycle management.

Finally, it is important to **maintain detailed documentation of the deployment process**, including any challenges encountered and solutions implemented. It is likely different components of governments will be responsible for securing their specific systems. Due to this separation, sharing lessons learned across the enterprise will be important for an efficient deployment process. Since this is a whole-of-government approach that requires coordination from all partners, updates should be regularly reported to stakeholders with these insights used to inform the broader deployment strategy.

Annex E-1: Case Study: Services Australia's Journey

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. By keeping up to date with modern cryptographic algorithms, Australia will be best placed to ensure we can keep our information safe and secure – 2023-2030 Australian Cyber Security Strategy

Services Australia, a critical government agency responsible for national payments and services, relies heavily on mainframes to process and store sensitive citizen data. With the looming threat of quantum computing potentially rendering current cryptographic methods obsolete, Services Australia recognized the urgent need to prepare for a PQC world.

Services Australia faced several challenges, including securing vast amounts of sensitive citizen data against future quantum threats; assessing and upgrading existing cryptographic systems; and, implementing quantum-safe encryption methods without disrupting critical services. The agency developed a comprehensive 4-step roadmap for quantum-safe readiness:

1. **Assess Pervasive Encryption Readiness:** Evaluate the current encryption status and prepare for implementing pervasive encryption on affected systems.
2. **Configure Trusted Key Entry (TKE) Workstation:** Implement secure master key management practices and prepare for quantum-safe key management.
3. **Install Unified Key Orchestrator (UKO):** Centralize and streamline application key management across the enterprise.
4. **Assess Quantum Safe Posture:** Conduct a thorough analysis of the current cryptographic landscape and develop a strategy for transitioning to quantum-safe algorithms.

The project is still in its early stages, but the expected outcomes include:

- Enhanced data protection through pervasive encryption
- Improved key management practices, reducing insider threat risks
- A clear roadmap for transitioning to quantum-safe cryptography
- Increased readiness for future quantum computing threats

The agency estimates significant cost savings in data breach prevention and a substantial reduction in potential GDP loss from quantum-enabled attacks. Early preparation for post-quantum cryptography is crucial for organizations handling sensitive data. A phased approach allows for systematic assessment and implementation of quantum-safe measures. Collaboration with experts in the field is essential for navigating the complex landscape of post-quantum cryptography.

Services Australia's proactive approach to PQC readiness sets a precedent for other Australian Government agencies and organizations dealing with sensitive data. By investing in assessment, planning, and implementation of quantum-safe technologies, the agency is taking crucial steps to protect citizen data in the face of emerging quantum computing threats.

Annex F: Ensure Future Resilience

[Crypto-agility] should…become a design criterion for new products - irrespective of the development of quantum computers. - German Federal Office for Information Security.

The cryptographic transition is not over once the algorithms are implemented. After deployment, governments must ensure that their systems are secure for long-term resilience. The most sustainable and effective way governments can do this is to implement a methodology for continuously assuring and tracking cryptographic use by government systems, and deploying cryptographic agility across those systems.

First, governments should adopt a robust monitoring framework that would allow them to **continuously track the performance and security of their post-quantum implementations.** Metrics might include processing speed, latency, resource utilisation, and system throughput. Using these metrics, governments can identify any areas that require adjustment to enhance the effectiveness of post-quantum cryptographic solutions. To ensure protection, regular security audits and vulnerability assessments will help to identify and address any weaknesses in the post-quantum implementations.

Second, governments must focus on **building crypto-agility into their systems.** Crypto-agility refers to the capability of a system to adapt its cryptographic methods swiftly in response to emerging threats or advancements in technology. This is crucial as cryptographic transition challenges are not a new problem. The world has frequently seen technological innovation outpace cryptographic security; advancements in quantum computers may pose the need for such adaptability.

To achieve crypto-agility, governments should apply a comprehensive approach that goes beyond simply updating encryption algorithms. This involves rethinking the cryptographic architecture to enable flexibility and rapid adaptation to future threats. Automation plays a critical role, allowing for the efficient management of cryptographic settings, keys, and certificates across various systems without manual intervention. Additionally, strong governance is essential, ensuring that cryptographic practices are consistent, well-documented, and able to evolve in response to new vulnerabilities.

By integrating these elements – robust monitoring frameworks and crypto-agility – governments can establish a resilient architecture capable of adapting security as technology and threats continue to evolve.