REF: 11062025

To DSIT

I used to own my own IT Company and whilst I'm not professing to be an Expert in the field of Quantum Computing (QC), because I sold business and consumer solutions for 10 years including Corporates, SME's and Public sector, I had been compiling some information on Security in Quantum Computing for a while.

I recently read the Cyber Governance Code of Conduct and perceived a threat that I believe IOT has in Quantum Computing. However there are serious implications also in the Digital Tech Sector as a whole, as I will outline.

Having looked up info on this, which had also been mentioned by **Amdea** where I picked up the Governments response to **Smart Secure Electricity Systems**. *More about that later in relation to IOT.* Now I note in the COC that there is nothing mentioned directly about QC, but that the concern is actually echoed in the National Cyber Security Centre (NCSC)'s guidance, which outlines a roadmap for transitioning to post-quantum cryptography (PQC) by 2035. The NCSC emphasises the necessity for organisations to begin preparations now to safeguard against future quantum threats.

I think that a bit more emphasis in the CoC to business about QC could have been mentioned but it's Quantum Resilience that's missing. However, the Training that is available nonetheless is to be commended.

In my humble opinion there is a real need for Government and Businesses to be hearing about Quantum Resilience in Data Storage regarding Digital Security Standards and I'm not sure just how aware the Government is on this subject. I've pulled together I hope, some very useful information for you to observe and perhaps consider because we're **all** impacted.

I'm engaged with DSIT already in Digital Inclusion (Mirka), and I have expressed other concerns of safety and legislation with (Mirka). I'm not satisfied yet that anything is being done about it with Mirka, which is worrying as the Charter IT Reuse Playbook is about to be released!

Anyway I hope the work below I've provided and points I've made can be looked at and I hope you can give me a response or some assurances as to my concerns. Particularly the IOT section. More devices than ever are being connected, and I would like to see more engagement between yourselves and OPSS-Dept of Business and Trade on these matters, I think there are some worrying gaps that may not have been identified, based on the content I'm supplying.

Best regards
Robert Alexander
CEO and Founder EEESafe & LocalitEEE

Introduction

As the UK Government moves to establish world-leading cybersecurity and AI safety frameworks, it must account for a looming threat: the vulnerability of today's encryption and data storage practices in the face of future quantum computing. Here I want to highlight the urgency and outline specific policy actions to ensure digital infrastructure remains secure, trustworthy, and future-proof. I provide references which I hope will prove helpful as much of this not only is beyond your knowledge, but I am no expert in the field of this, but aware enough to draw concerns.

The Quantum Risk

"Quantum computers will be able to break the encryption that protects today's internet."
— **National Institute of Standards and Technology (NIST), USA**

Encryption underpins digital trust across sectors: healthcare, energy, identity, and financial systems. Current standards like RSA and ECC rely on mathematical problems that classical computers struggle to solve — but quantum computers will solve them rapidly.

Shor's algorithm, once implemented on a sufficiently powerful quantum machine, will render most asymmetric encryption ineffective. This means:

Encrypted health records, government databases, and digital identities could be exposed.

Secure communications could be retroactively decrypted.

Harvest Now, Decrypt Later

"Adversaries can harvest encrypted data today, store it, and decrypt it once quantum computers become viable."
— **European Union Agency for Cybersecurity (ENISA)**

This strategy is already underway by state-level actors and cybercriminals. Even if data is safe now, it may not remain so — particularly damaging for long-lived data such as:

- Medical histories
- Smart infrastructure records
- Legal and regulatory logs
- Appliance and IoT histories

Current Data Storage Is Not Ready

Most storage systems in the UK — cloud or local — are not **crypto-agile** (i.e., able to shift to new cryptographic methods without rebuilding infrastructure). This is especially true for:

- Appliance IoT ecosystems
- Healthcare record systems
- Municipal smart devices and services

Many storage formats embed hardcoded encryption assumptions, making post-quantum upgrades costly and time-consuming unless planned for **now**.

A Call to Government

To maintain leadership in digital trust, the UK must include **quantum resilience in its digital security standards** and Codes of Practice. Recommended actions include:

- **Prioritise crypto-agility** in new software and storage standards
- **Adopt Post-Quantum Cryptography (PQC)** being standardised by NIST and the UK's NCSC
- **Create compliance requirements** for regulated sectors (e.g., health, utilities, smart cities)
- **Develop guidance and grants** for SMEs to upgrade to quantum-resilient systems
- **Contribute to international collaboration**, including ISO/IEC and ETSI PQC workstreams

---

Relevant Developments

- **NIST (USA)** selected four PQC algorithms for standardisation in July 2022.
- **UK's NCSC** is advising organisations to prepare for "Y2Q" — the quantum break event.
- **ISO/IEC JTC 1/SC 27** is actively developing standards for post-quantum security.

Why This Matters Now

The arrival of quantum threats is not a matter of *if*, but *when*. National data, once exposed, cannot be "re-secured" retroactively. The ability to trust digital systems — especially those driven by AI and IoT — is foundational to:

- National resilience
- Economic confidence
- Digital sovereignty

Conclusion
The UK has a rare opportunity to lead globally on this issue — not just in AI safety, but in the long-term security of its digital economy. Post-quantum readiness is not an optional upgrade; it's a necessity.
"It's not about panicking now — it's about building wisely today."
— **Dr. Michele Mosca**, co-founder, Institute for Quantum Computing
By integrating quantum-safe principles now, we can ensure that the systems we build today will still be secure tomorrow.

NOTE: I think it's worth pointing to this Shorter Video from Thales Mike.
This is a much better video and really helps to support my points.
https://www.youtube.com/watch?v=vTSbeL0q530

Ensuring Repair Access, Safety and Cyber Resilience in the Age of IoT and Quantum Computing

Introduction

EEESafe welcomes the opportunity to contribute to the UK Government's ongoing development of cybersecurity, IoT policy, and digital safety standards. As a social enterprise working at the intersection of appliance safety, repair training, and community resilience, we believe it is vital to address emerging risks associated with the growth of smart (IoT-enabled) appliances and their implications for people, place, and planet. In short, our Global Sustainability.

1. The Quantum Risk & Insecure Data Futures

As quantum computing evolves, current encryption methods used in both storage systems and IoT devices will become vulnerable. Most smart appliances rely on classical cryptographic schemes (e.g., RSA, ECC), which are expected to be broken by future quantum capabilities. This places sensitive consumer, appliance, and usage data at long-term risk of breach.

EEESafe urges the government to ensure that IoT and data governance strategies include post-quantum encryption standards and crypto-agile data storage frameworks.

2. IoT-Driven Repair Monopolies Undermine Resilience

Manufacturers increasingly use software locks and digital restrictions to limit who can repair smart appliances. This centralizes control and marginalizes the role of independent repairers, especially at the local level. These restrictions undermine affordability, environmental sustainability, and economic resilience.

The ability to repair and reuse products locally is critical for Net Zero targets, circular economy goals, and social equity across UK communities. Whilst Control of Repair is in the hands of IOT Portals, the Wider Independent Repair network is in jeopardy, where the lowest possible costs of repair is the only way to drive sustainable change. Supporting Manufacturers in PAAS models and leasing, is only going to add costs to household budgets. An "Everything Subscribed" model, will never work. It's been tried in the past and failed. "Radio Rentals". It profits the Richest and leaves the poorest with no choice and takes away local economic strength and reduces local skills development. Our own Model offers an alternative.

3. Safety Risks in Unregulated Repairs

While EEESafe supports the principles of the Right to Repair movement, we must also address the associated safety risks. Today, consumers often buy second-hand electrical goods online without knowing who repaired them or whether it was done safely. This creates potential hazards in the home and under current law, makes the last person to repair anything, open to prosecution and potential jail, if any product is the subject of an accident, fire or fatality. A subject of concern raised at the recent Manufacturers Sustainability Event, which a few Government Sectors in attendance heard.
We believe that **Right to Repair** must be complemented by a **"Right to Know"** — a verified history of an appliance's repairs and who carried them out, which is what we offer.

4. EEESafe's Digital Twin & Community Repair Solution

EEESafe is preparing to launch the UK's first community-led Appliance Safety Register, underpinned by Digital Twin technology and a Digital Inclusion solution. Each appliance will be registered with a unique ID, storing:

- Repair history
- Replacement parts
- Safety checks

Identity and qualifications of the repairer or none at all. This system promotes safety, traceability, and consumer trust. Our goal is to establish a public-facing standard for appliance repairs — akin to Gas Safe — empowering citizens while supporting local repair ecosystems and reducing waste.

5. Recommendations

- To align with the UK's ambitions for a secure, innovative, and equitable digital economy, EEESafe recommends:
- Integrate post-quantum cryptographic standards into all IoT cybersecurity and data storage codes of practice.
- Enforce design standards that enable safe repair and maintenance by independent, accredited community repairers.
- Support national digital safety registers for appliances, including repair history and repairer identification.
- Embed "Right to Know" principles alongside Right to Repair legislation to ensure consumer safety.
- Fund community-based training and accreditation for local repairers through social enterprise and nonprofit networks.

Conclusion

EEESafe stands ready to collaborate with policymakers, regulators, and industry stakeholders to ensure that digital innovation in the appliance sector serves both consumer needs and societal good.
We believe our Digital Twin Appliance Register can be a national exemplar — a model for balancing cybersecurity, sustainability, and local empowerment in the age of IoT and quantum risk