# SIF Beta Round 5 Project Registration

### Date of Submission

Sep 2026

### Project Reference Number

10166255

## Initial Project Details

### Project Title

Network Security in a Quantum Future – Beta

### Project Contact

innovation@neso.energy

### Challenge Area

Enhanced system visibility and control

### Strategy Theme

Optimised assets and practices

### Lead Sector

Electricity Transmission

### Project Start

01/08/2026

### Project Duration (Months)

19

### Lead Funding Licensee

NESO - National Energy System Operator

### Funding Mechanism

SIF Beta - Round 5

## Collaborating Networks

SP Energy Networks Distribution

SP Energy Networks Transmission

National Gas Transmission PLC

## Technology Areas

Cyber Security

Resilience

Stakeholder Engagement

System Security

## Project Summary

As UK Critical National Infrastructure, the energy system must be secure against malicious cyberattacks.
Emerging quantum computing technologies will enable attackers to break currently secure encryption and open significant new attack vectors. To ensure resilience, energy networks must therefore consider quantum threats in their cybersecurity strategies; however, understanding quantum impact requires highly specialist knowledge.

After successfully prototyping innovative risk management approaches to assessing the quantum threat to the energy network in Alpha, the Network Security in a Quantum Future (NSiaQF) Beta will develop quantum threat management tools to map quantum threats to energy system assets and prioritise appropriate mitigations.

## Add Preceding Project(s)

10103996 (2) - Network Security in a Quantum Future

10129418 - Network Security in a Quantum Future - Alpha

## Add Third Party Collaborator(s)

Cambridge Consultants

University of Edinburgh

## Project Budget

£7,211,187.00

## SIF Funding

£6,191,000.00

# Project Approaches and Desired Outcomes

## Animal testing (not scored)

- ○ Yes
- ◉ No

## Solution statement and solution focus

Problem
The grid is facing an unprecedented convergence of new technologies, pressures, and threats. The control room of the future will depend on trustworthy data, software and communications from multiple organisations to ensure resilience and stability. This means authenticating data sources, establishing encrypted pathways between digital/IT and cyber-physical systems, and validating that all software and firmware are from trusted suppliers. These functions depend on secure cryptography.
Quantum computers will pose a major threat to the cryptography used by the energy system. A quantum computer will reduce the time needed to "break" cryptographic algorithms from over 1,000 years to less than 8 hours. Once broken, attackers could access, send, or manipulate data; pose as legitimate systems; or even execute their own software on grid assets causing potentially catastrophic disruption.
The UK's National Cyber Security Centre (NCSC) has issued guidance that high-priority Critical National Infrastructure (CNI) systems (which includes energy networks) must be migrated to quantum-resistant cryptography (post-quantum cryptography, or 'PQC') by 2031, with other systems migrated by 2035.
The energy sector therefore needs an appropriate and proportionate approach to effectively migrate to PQC in a timely manner. This approach must be well-planned to avoid costly, reactive "rip and replace" strategies. PQC will be critical for ensuring security and accuracy of control room data and functions; and for protecting the broader cyber-physical estate of energy network operators, given the central role of the control rooms as communications hubs.

Key challenges:
Quantum technology is developing rapidly, and the threat horizon is evolving with it. Network Security in a Quantum Future (NSiaQF) Discovery phase confirmed a significant threat within ~10 years (i.e., within current asset lifespans).
Understanding quantum computing research and mapping it to meaningful, actionable information for energy network security teams requires significant specialist knowledge that is in short supply.
The complexity, scale, distributed nature, and long asset lifetime of energy assets make PQC migration planning highly complex. Protecting against the quantum threat must meet the dynamic needs of the future energy network, integrating with cybersecurity BAU, while ensuring grid operations remain cost-effective and resilient.

Solution
Our proposed solution is to develop two groundbreaking interconnected PQC decision-support tools, which NSiaQF Alpha developed to proof-of-principle:
Quantum Threat Tracker (QTT): models quantum developments to identify the threat horizon and cryptographic vulnerabilities.
Quantum-Aware Risk Manager (Q-ARM): applies these insights to energy network assets and articulates/prioritises the risks for energy network cybersecurity specialists for effective migration planning and risk management.
NSiaQF Beta will develop both tools to Minimum Viable Product (MVP) to support the network's migration to PQC in a cost-effective, scalable, explainable and repeatable way.

Challenge Alignment
NSiaQF is aligned to the objectives of Challenge 5: Enhanced system visibility and control, by: ensuring future resilience of trusted infrastructure for real-time system monitoring, adaptive grid control, digital automation, AI-driven analytics and advanced decision-support tools, providing visibility of quantum risks to control room cybersecurity teams.
NSiaQF will guide deployment of appropriate, proportionate cybersecurity mitigations that are vital to the success of new control techniques in an ever-more complex grid environment. Securing the communications vital to control room operation will also protect enhanced operator, generator and consumer coordination.
Users
Energy network security teams will be the primary users. To ensure broad applicability beyond NESO, NGT and SPEN have therefore been added as partners in Beta.
A Quantum-Security Advisory Council (Q-SAC) will also be formed based on the stakeholder map created in Alpha. This will be used to further broaden stakeholder input, advising on requirements and sector needs and concerns.

Secondary users:
Quantum computing researchers.
Cross-sector policymakers concerned with potential quantum security impacts.

Other Funding
None.

## International Collaboration (not scored)

No confirmed international collaboration at present. Potential international engagement is being explored and may develop during the project

## Trusted Research And Innovation

UKRI's TR&I Principles
Network Security in a Quantum Future (NSiaQF) does not relate to UKRI's TR&I Principles.
Sensitive Information
All sensitive information will remain with the originating energy network and will not be shared.
NS&I Act
There will be no acquisitions in this project.

## Innovation justification

**Meeting Challenge Requirements**
NSiaQF's is aligned to Challenge 5: Enhanced system visibility and control, by enhancing resilience of the GB energy sector to emerging quantum-enabled cyber-attacks through novel software and computing tools:

- NSiaQF's tools will enable security against quantum threats for the technologies required for real-time system monitoring and grid visibility, and facilitate more direct self-healing and resilience technologies by ensuring data security.
- Automating aspects of quantum risk management will facilitate trusted communication and coordination between grid operators, generators, and consumers, directly contributing to grid resilience.

**State-of-the-art**
No current tools can reliably support informed decision-making about quantum threats to energy networks:

- Discovery and modelling tools lack data on quantum-enabled attacks, detecting theoretical vulnerabilities, but, critically, they cannot estimate risk.
- Quantum threat characterisation is primarily from academic sources that don't track evolution or update dynamically.

Innovation

NSiaQF goes beyond incremental innovation to fill these gaps and improve energy sector resilience:

- Characterising and articulating quantum risks: NSiaQF tools will produce novel, evidence-based estimates of quantum risk, combining 'time-to-attack' (time until sufficient quantum computing resources become available to attackers) with 'time-of-attack' (time required to initiate and execute a quantum attack). NSiaQF tools will generate trusted and actionable quantum threat reports for energy system cryptographic protocols that won't require quantum expertise to understand, including communication of risk evolution over time and the associated uncertainty.
- Embedding quantum risk management into BAU: In line with NCSC guidance, NSiaQF's repeatable, evidence-based approach will support well-planned, cost-effective PQC migrations, aiding trade-off decisions and prioritisation as part of BAU.
- Modelling energy network assets: Beta will continue development of a standardised energy asset library, adding new asset models. Our transparent, modular approach will enable standardisation and risk reduction and streamline adoption by networks.

**Counterfactuals**
Alternatives are expensive, risky, or insufficient:

1. Manual approaches: The number/complexity of interconnected energy assets make manual prioritisation for PQC migration impractical, risking delays in addressing vulnerabilities. Also requires hard-to-access expert quantum threat knowledge.
2. Reactive approaches: Ad-hoc PQC migration approaches would increase up-front expenditure and total cost of ownership due to early, unnecessary upgrades and/or incorrect prioritisations.
3. Other tools: Do not deliver the information or functionality required.

**SIF Learning and Stakeholder Input**
**Alpha learnings:**

- Automated identification of quantum risks for modelled energy assets.
- Modelled quantum computing methods to predict when specific algorithms and key lengths will be vulnerable.

Beta will build on these, and address challenges identified during Alpha:

- Manage the highly variable quantum implementation approaches pursued by corporations and national laboratories and the resulting impacts on the risk assessment.
- Capturing and communicating uncertainty from quantum research.
- Making the QTT an attractive open-source tool to capture quantum information from experts.

Our comprehensive Alpha engagement strategy ensured NSiaQF will be valuable to the sector through:

- Soliciting feedback via industry presentations and 1-2-1 discussions with networks.
- Sharing a 'clickable demo' of the tool.

We have not identified other network-funded projects exploring quantum threats to the energy sector.

**Readiness Levels (Alpha-\>Beta)**
Beta will make the tools production-ready, enhancing quality, accuracy, reliability, and trustworthiness.
TRL4-\>TRL7
IRL3-\>IRL6
CRL3-\>CRL8

Scale
NSiaQF will support the sector in managing quantum risk by developing high-quality, reliable, scalable tools for potential use by all GB energy networks. To this end, NSiaQF Beta adds SPEN (Distribution and Transmission) and National Gas as partners and creates a Quantum-Security Advisory Council (Q-SAC) to ensure industry alignment and continued working-in-the-open.

SIF Funding
Quantum cybersecurity threats pose a nationally significant, industry-wide challenge. The complexity and interconnectedness put NSiaQF out-of-scope of normal energy network strategic planning and other network funding mechanisms. SIF has enabled a structured response (developing a process, then a tool) through sector-wide collaboration.

## Impacts and benefits selection (not scored)

Financial - future reductions in the cost of operating the network

Environmental - carbon reduction – indirect CO2 savings per annum

New to market – products

## Impacts and benefits description

For all the SIF benefits identified in the Impacts and Benefits selection question, you must:
1 - Describe what the current position (pre-innovation baseline) is, and the metrics that will be used to report on these
2 - Provide an initial forecast of the quantified or qualified cumulative net benefits to Energy consumers to be realised, calculated at a network partner level, should the innovation be implemented into business as usual
3 - Describe, quantify, or qualify any benefits already realised through project delivery

Current Situation
Quantum-enabled cyberattacks against GB energy networks will be possible in 8-10 years. In the pre-innovation Baseline, energy networks take a passive approach to preparation, relying on vendors to deliver quantum-related security upgrades. This is more realistic than assuming they would "do nothing", which would be a dereliction of networks' license conditions and NCSC

guidance.
Under Baseline, migration delays and poorly prioritised upgrades would increase the risk of quantum-enabled cyberattacks, leaving energy networks vulnerable for an unacceptable time period.
Our CBA assesses overall benefits of NSiaQF (Tool Development Scenario):

- 30-year NPV (compared to baseline): £82.8Bn
- Costs: £0.85Bn over the full forecast period to 2054, of which £6.19Mn for Beta project funding
- 3-year break-even

**NSiaQF Benefits :**

**Financial** - future reductions in the cost of operating the network
Avoided cost of quantum-enabled cyberattack: NSiaQF Discovery estimated the cost at tens of billions. The impact would be so severe that the benefit of anything that mitigates the risk is significantly greater than can be expressed by NPV calculations alone.
Metric: Avoided cost of cyberattack; conservatively, £19.4Bn by 2054.
Reduced cost of cybersecurity expenditure: Requirements for cybersecurity expenditure will reduce over time, as NSiaQF enables operators to address highest-impact mitigations first, spread costs over time, and plan upgrades cost-effectively by using up-to-date quantum information.
Metric: Savings vs counterfactual cybersecurity spend. Cumulative cybersecurity spend in NSiaQF scenario will drop below Baseline from 2036 onwards; by 2054, savings will be £38.5Bn.

**Environmental** - carbon reduction -- indirect CO2 savings per annum
Avoided increase in CO2 emissions from quantum-enabled cyberattack: In a blackout, networks would rely more on gas power plants. Would save ~658,520 tCO2e in emissions by 2054.

**New to Market -- Products**
Introduction of Q-ARM as a tool for network operators: There is currently no available tool for network operators to easily assess and prioritise energy system assets for quantum vulnerability. Q-ARM will be commercialisation-ready at the end of Beta.
Metric: Number of operators adopting the tool.
Creation of QTT as a Resource for Quantum and Cybersecurity Development: There is currently no common approach for the quantum community to share information on quantum impacts on cybersecurity. In Beta/post-Beta, QTT will enable valuable collaboration by quantum experts, feeding directly into Q-ARM's energy asset risk assessments.
Metrics: Number of active QTT contributors; number of code downloads.

**Other Benefits**

De-risking cybersecurity of energy network assets and systems in the post-quantum world
A reduced risk of quantum-enabled cyberattack brings societal benefits:

- Reduced number of customer interruptions: Based on expected number of customers interrupted from a national/regional (5% of GB) attack: avoiding ~24.1m interruptions.
- Reduced customer minutes lost: Based on the same expected number of customers interruptions, multiplied by average disruption length (7-days national; 3.5-days regional): avoiding ~233Bn minutes lost.
- Avoided cyberattack-linked fatalities: Based on expected number of fatalities: saving ~1,195 lives.
- Avoided attack-linked injury: Based on the expected number of major injuries: avoiding ~2,390 injuries.

**Alternative Approach**
We evaluated an alternative scenario, Rip-and-Replace, where operators undertake full-scale pre-emptive replacement of their cryptographic assets to be quantum-safe. While more beneficial than Baseline, it still delivers fewer financial, environmental and societal benefits than the NSiaQF tool scenario (lower 30-year NPV £39.3Bn), with higher up-front costs (£12.4Bn).

**Already-Realised Benefits**

- Developed clear and innovative approach to characterising attack types enabled by quantum computers, linked to asset types.
- Drawing on previously unconnected research sources to create unique mapping tables that enable automated quantum risk discovery: a definitive mapping of mathematical problems; a unique mapping of quantum attack and mitigation types; and a mapping of quantum-enabled attacks to system security properties.
- QTT already created as an open-source tool to start engaging the quantum community.

## Teams and resources

Who will be involved with the delivery of the Project during the Beta Phase?
No additional resources, equipment or facilities will be required for Beta.

**Project Team**
Existing Partners
NESO (lead)

NESO, the GB Energy System Operator, will steer the project to produce useful outcomes for NESO and the wider energy industry. NESO's Head of Energy Sector Security, Sarah Hadfield, and her team will provide detailed functional requirements, identify relevant use cases and undertake user testing. Alongside overall project management, NESO is responsible for project governance, subcontracting the software developer and ensuring Q-ARM is compliant with NESO's system requirements, wider industry stakeholder engagement and commercialisation/BAU transition planning.

**Cambridge Consultants (CC)**
CC is a deep-tech engineering consultancy working across multiple industry sectors, with departments specialising in both cybersecurity and quantum computing. CC will provide the technical leadership within the project for both Q-ARM and, in collaboration with UoE, QTT. CC will also leverage their business model development experience to support NESO with the long-term commercialisation plans.

**University of Edinburgh (UoE)**
UoE is a leading research university with specialisms in quantum computing, power systems, and decision analysis. UoE hosts the Quantum Software Lab, a research centre focused on exploiting quantum computers to solve problems beyond the reach of classical machines. UoE will lead the development of the QTT, using their experience in cryptographic quantum computing, quantifying uncertainty and ensuring a clear mapping to energy networks.

**New partners**
National Gas Transmission and Scottish Power Energy Network are new partners for Beta who increase NSiaQF's energy sector stakeholder reach. NESO has existing relationships with both new partners.
Both new partners will advise on:

- Functional requirements, to ensure Q-ARM is usable across energy networks.
- Their system requirements, to ensure Q-ARM's scalability.

**National Gas Transmission (NGT)**
NGT, a part of National Gas, owns and operates the GB gas National Transmission System (NTS). NGT will broaden Q-ARM's scope for gas networks.

**Scottish Power Energy Network (SPEN)**
SPEN is the company responsible for delivering electricity to homes and businesses in parts of Scotland and Wales. SPEN's team covers both electricity transmission and distribution, and so will advise on requirements for both electricity Distribution Networks (DN) and Transmission Networks (TN).

**Other Parties**

**Quantum Security Advisory Council (Q-SAC)**
Additional stakeholders will be engaged through a Quantum Security Advisory Council (Q-SAC). Building on Alpha's successful engagement campaign, we have already identified the following individuals from senior stakeholders:

- Anne-Claire Blet, Deputy Director of the National Quantum Computing Centre (NQCC)
- Sarah Hadfield, ERG-CC
- Aliabbas Bhamani, ERG-CC

We are hoping to include additional stakeholders in the Q-SAC once funding is confirmed; there are ongoing discussions with National Cyber Security Centre (NCSC) and Ofgem.

In project, we aim for the Q-SAC to also include multiple other GB networks. We will also look to include consumer groups to ensure the voice of the consumer is considered, though this will require careful consideration owing to the highly technical nature

of the challenges.

The Q-SAC will provide additional guidance and insight on the requirements for the tools to ensure they are appropriate and usable across GB energy networks and beyond. The draft Q-SAC Terms of Reference (ToR) are available on request.

**Subcontractors**
To ensure best value for money for consumers, development of Q-ARM will utilise a third-party subcontractor, selected via the NESO D&D framework (current costing is capped estimate). They will operate under the instruction of CC and NESO.
Using the NESO D&D Framework allows us to run a mini-tender to ensure good value, while also simplifying the contractual process. Details of NESO's D&D Framework are available on request.

# Project Plans and Milestones

## Project management and delivery

**Project Management Approach and Governance**

The project will be split into four work packages and utilise shared project resources, research and governance. A risk register and a full set of deliverables and milestones for each work package are included in the PMT.

**WP1: Project Management, Governance and Dissemination (NESO lead)**
NESO will assign a dedicated project manager, responsible for project coordination, governance and dissemination, and appoint a Resilience and Energy Management lead to ensure alignment with energy security requirements. Regular progress meetings with partners and the creation of a Q-SAC (Quantum Security Advisory Council) will be used to review project and technical progress, alignment of outputs and risks.
Key Tools:

- MS Project
- SharePoint
- NESO PMO Framework

**WP2: Quantum-Aware Risk Manager (CC lead)**
Development and wider user testing of an MVP software tool for identifying and prioritising mitigation strategies against quantum risks to energy networks. This will commence with a waterfall requirements capture and architecture development, followed by an agile sprint-based software development, concluding with pre-deployment and wider user functionality testing.
Key Tools/Processes:

- GitLab Kanban
- Sprint Review/Planning Meetings
- SCRUM Methodology

**WP3: Quantum Threat Tracker (UoE lead)**
Development program to scale and improve the quality, accuracy, uncertainty and usability of the QTT; and to include in QTT assessment of the uncertainty in timeline of technology and algorithm development. Development follows a waterfall structure, including reviews in combination with WP2 sprint reviews to ensure aligned development, continuing the collaborative approach from Alpha.
Key Tools:

- GitLab Kanban

**WP5: Commercialisation (NESO Lead)**
Developing the commercialisation strategy for long-term support into BAU by defining support requirements, the commercialisation model and developing a viable approach to adoption by other energy network adopters. In this workstream we will also review, validate and refine the cost-benefit analysis for the tools. In addition, this workstream will include development of a framework to assess benefits of the tool post-Beta, including relevant metrics and benefit criteria.
Stage Gates

- Software Architecture Complete (Month 6): Requirements captured across all workstreams; technical architectures proposed ahead of software coding.
- Beta Software Tool Development Complete (Month 13): Q-ARM ready to move to pre-deployment testing on energy network partner system(s) to enable wider user functionality testing. QTT second major release to open-source community. Defined commercial approach for long-term tool support and maintenance.

**Risk Management**
Risk Management will be a continuous process, monitored and actively maintained by the PM using an Identify, Assess, Control, Record approach. Risks will be a standing item at the weekly project management meetings. Mitigation activities, owner assignment and progress will be discussed. Escalation to senior management will be utilised as required.

Key risks

- R2: Aggressive project timelines for full development cycle to meet imminent user needs.
- R4: Diverse functional and deployment requirements across the different types of energy networks.
- R7/R8: Security and sensitivity of the information used by the tools after deployment.
- R12/R18: Long term support required to ensure tools remain relevant and fed with up-to-date information into BAU.

**Dependencies**
The project has been designed to reduce dependencies across work packages as far as is reasonable. Primary dependencies are between WP2 and WP3 and are reflected in the project plan.

**Interruption and Customer Impact**
The project itself will not impact access to energy services nor require any direct or indirect supply interruptions, as it will not involve direct interaction with the energy network equipment or markets. Conversely, it is designed to develop tools to help ensure that consumers have ongoing access to the energy services and connections they require through the effective use of risk mitigation for quantum threats.

## Key outputs and dissemination

**Achievements and Main Outputs**
At the end of Beta, we will have built and tested two software tools to Minimum Viable Product (MVP):

At the end of Beta, we will have built and tested two software tools to Minimum Viable Product (MVP):

- The Quantum-Aware Risk Manager (Q-ARM), which provides quantum risk assessments for energy systems.
- The Quantum Threat Tracker (QTT), which models the latest quantum technology information.

These will be mature enough for energy network 'early-adopters' to run approvals testing and begin their transition to Business-as-Usual (BAU).

The tools will be validated on at least 10 relevant energy network test cases (building on the two already validated in Alpha) covering needs and interests across different types of UK energy networks (electricity/gas, transmission/distribution), and will have been tested by partner energy networks.

**Main outputs:**

- Q-ARM [CC-led]: Development of a bespoke software tool, including a comprehensive energy asset library for modelling risk assessments; a set of associated quantum-enabled Tactics, Techniques and Procedures (TTPs); and a set of potential mitigation strategies.
- QTT [UoE-led]: Further development of QTT's capabilities, including improved methods for estimating quantum timeline uncertainties; improved data accuracy (accounting for rapid developments in quantum algorithms); and features to support development of an open-source community, including clear policies and processes for integrating community inputs.
- Commercialisation [NESO-led]: A strategy for ensuring the long-term viability of the tools, including: full commercialisation plan; establishing of a robust, sustainable QTT open-source community (building on Alpha); quantification of NSiaQF benefits by validating and refining the Cost-Benefit Analysis (CBA) and business case; and definition of a framework for measuring post-project benefits.

**Additional Outputs and Dissemination**
The following outputs will also help disseminate learnings [including owners]:

- SIF Governance: Annual Progress & Final Project Report; Show-and-Tell. [NESO/CC/UoE]
- Reports shared on ENA Smarter Networks Portal and learning promoted to the sector. [All]
- The Q-SAC, and workshops with Energy Resilience Group (ERG) and/or other energy industry body members, focussing on stakeholder input and demonstrating the developed tools to increase energy industry suitability. [All].
- Hosting two open-to-all, but primarily for the quantum community, QTT user conferences (TBD but Q4-2026 and Q4-2027 planned) to build confidence and interest in QTT. [CC/UoE/NESO]
- Presentation of QTT at relevant academic and quantum computing conferences, for dissemination and community building.

[UoE/CC].

- Participation in the annual SIF community forum and, where possible, Energy Innovation Summit. [All]

Project outputs will also be disseminated across the public domain in accordance with SIF Governance requirements (including the 60-second project launch and completion videos, and end-of-phase show-and-tell).

**Competitive Markets**

The key project information will be openly shared with all energy networks, ensuring key knowledge from Beta is available so all energy sector stakeholders can benefit. To this end, NESO will provide free licenses to use Q-ARM to all GB energy networks that want it.

Open knowledge sharing should also facilitate the development of alternative vendor solutions, ensuring there is competition for the solution itself. The open-source nature of QTT (a key information resource for innovators) will also facilitate and inspire additional products and services.

More broadly, NSiaQF is designed as an enabler of increased market competition, rather than to undermine it. NSiaQF enables energy network security teams to discuss the quantum threat with supply chains in an informed way. NSiaQF will therefore ensure competitive procurement processes are as secure as possible, enabling competition and innovation within energy markets.

**Collaborative working**

NSiaQF will continue the collaborative working approach from Alpha, with partners completing regular shared technical reviews of work completed. This will be extended to new partners SPEN and NGT, and to all partner's IT, commercial and procurement teams to ensure sustained support beyond Beta.
The proposed Quantum Security Advisory Council (Q-SAC) will also ensure the project continues working-in-the-open with stakeholders.

# Commercials

## Intellectual Property Rights (IPR), procurement and contracting (not scored)

**Intellectual Property Rights (IPR), procurement and contracting**
Following the rejection of NESO's previous NSiaQF application, we can confirm we will deviate from the default SIF Governance IPR position as detailed below:

**Q-ARM**
Full Foreground IP ownership (including code, documentation and all rights) will rest with NESO at project conclusion, rather than Cambridge Consultants (the Q-ARM's development lead). Please see page 1 of the Appendix for the proposed model for the Q-ARM IP.

Acknowledging the feedback from the previous application, this position ensures that best value will be delivered to consumers who, through SIF, are investing in the development of Q-ARM. However, owing to the type of organisation NESO is, NESO's approach to supporting the enduring Q-ARM solution post-Beta will be to appoint a third party to provide software maintenance for NESO.
The licensing of the software to third parties needs to balance:

- Paying for this internal support;
- making Q-ARM available for other networks to use; and,
- exploiting the software beyond the GB energy system.

This creates many questions that will be answered in the project (task 4.1); however, our initial positions are:

- NESO holds the Q-ARM Foreground IPR and acts as the Q-ARM custodian to ensure best value is delivered to consumers.
- Other GB energy networks will be granted a free license for use of the software. However, they will bear all their own set-up and support costs. (A separate arrangement for each network with NESO's own support partner will be possible.)
- To other industries (GB and International), licenses will be granted for development of industry-specific versions (e.g. other Utilities, telecoms) to external third parties under fair and reasonable terms.

Initially, and depending on their interest, we would expect to grant CC a non-exclusive licence for exploitation outside of the GB energy system on terms that take fair and reasonable account of CC's contribution to the project and to the creation of IP.

We believe that this arrangement recognises the contribution and expertise provided by partners in developing Q-ARM while also achieving best value for consumers. However, in keeping with NESO's status, assessments of costs, benefits and value for money will be made by NESO in all decisions.

**QTT**
QTT will be open source and so will be accessible to all, though foreground IPR ownership will rest with University of Edinburgh and CC for contractual purposes. These IP owners acknowledge and commit to the continuation of QTT as a freely accessible, open-source product available under the standard MIT License.
To remain useful, QTT will require a community of contributors from the quantum computing world, which will require some community management. In-project, QTT community management will be distributed between UoE, CC and NESO.
Post-Beta arrangements for maintaining this QTT community management will be agreed during the project (Task 4.2). This community support role has no bearing on QTT IP ownership.
Appendix Page 2 shows the open-source operation of QTT.

**In-project Procurement/Contracting**

We do not anticipate running any competition as part of the Beta project.
Note that, to avoid confusion, where this application makes reference to a "support provider" who will maintain and update Q-ARM for NESO in Business-as-Usual, this provider will be selected post-Beta.

**Subcontractor Selection**

As per Q10, NESO will subcontract a software developer to build Q-ARM under NESO and CC's instruction. They will be selected using the NESO D&D Framework before project commencement.

**Subcontractor TBD**

- Role: Development of Q-ARM under CC and NESO direction.
- Justification: Subcontracting via the NESO D&D framework ensures best value for consumers.

## Commercialisation, route to market and business as usual

**Commercialisation Plan**

WP4 will refine and finalise our commercialisation plan. Provisionally:

**Q-ARM:**

- Foreground IP owned by NESO. Centrally held and managed by NESO who act as custodians.
- Q-ARM requires ongoing maintenance, updates, oversight, etc. NESO would be responsible for this post-Beta for its own deployment of Q-ARM, but would select a third-party support organisation via tender. Self-funded by NESO.
- NESO grants licenses for use to energy networks and exploitation/development to others, as appropriate.
- Separate instances hosted by each network at their cost and to ensure information security.
- Initial route-to-market: Internal NESO deployment then GB energy network dissemination.
- Expansion (non-GB energy networks & other national & international industries) via granting exploitation licenses with non-exclusive FRaND access to project partners (recognising their contribution in-project) and others.

**QTT:**

- QTT will be open-source, hosted on an open-source repository. Core Foreground IP shared between CC and UoE.
- Held as open-source (MIT License). IP owners commit to keeping QTT open-source and available for all.
- Requires ongoing oversight, maintenance, and community engagement to maintain utility. CC, UoE and NESO will share these responsibilities, setting up a governing organisation and appointing designated community management post-Beta.
- Funding: self-funded by each organisation.

**Partner Commercial Readiness**

CC and UoE are well-placed to support both the QTT community engagement/events and assist NESO in developing the Q-ARM commercialisation plans:

- CC provides engineering/IT development services to enterprise and public sector clients, productising and commercialising technology innovations.
- UoE support commercialisation through its established IP commercialisation function and Quantum Software Lab.

**Senior Sponsorship**

Our NESO senior sponsor, Deborah Petterson (Director of Resilience and Emergency Management) has confirmed commitment to NSiaQF. Project sponsor, Sarah Hadfield (Head of Energy Sector Security), has been an active supporter from inception. They will continue to ensure:

- NESO's cyber teams support the project.
- Project outputs are relevant and valuable.
- Active engagement with energy networks, stakeholders and the Q-SAC.

**Path to BAU**

Post-Beta, the goal is for Q-ARM to be part of energy network operators' BAU cybersecurity planning toolkits, providing decision support for risk management.

Post-Beta, NESO will need to engage a third-party support organisation to provide ongoing enhancement, support and maintenance for NESO. Within Beta, we will design the competitive selection process for this support provider, enabling Q-ARM to enter NESO BAU following our productionisation process.

More detail on NESO's path to BAU process is provided in the Appendix, but WP4 will:

- Develop the support provider specifications and requirements.
- Conduct final productionisation plan design review and approval.
- Conduct an Impact Analysis to identify training, capacity, and processes changes.

Develop the commercial model further, validating it with partners, the Q-SAC and networks.

Individual networks will be granted a license but will need to cover their own set-up and maintenance costs. Note they would be free to use the same support provider as NESO, which may bring cost savings, but this is not a requirement.

**Competitive Markets**
NSiaQF will not undermine the development of competitive markets; indeed, NSiaQF is intended to ensure that current energy markets remain both competitive and secure. Trust in the transactional process is key to NESO (and other networks) operating markets in a fair, transparent and open way.

Conscious of the risk that NESO owning the Q-ARM IP might lock us into one service, we will guard against this via transparency and openness with project findings and results, sharing the development and learnings. This will ensure networks can benefit from the information/findings, and other suppliers can offer competing solutions.

Furthermore, QTT (the engine that drives the innovation) being open-source means it can be a platform for others to develop new applications, leveraging and maximising the value of NSiaQF for consumers

## Policy, standards and regulations (not scored)

**Policy/Regulation/Standards Barriers**

There are no policy/regulation/standards barriers that would impede this project for its duration.
However, there are two aspects of UK regulations and UK government guidance that this project needs to be conscious of, and that may impact the final tool once deployed:

- The way the tools themselves support compliance with obligations or guidance from the technical authority for cyber-security in the UK, the National Cyber Security Centre (NCSC).
- The regulatory requirements and standards for the deployment of software onto the networks of organisations supporting critical national infrastructure (e.g., the Cyber Security and Resilience (Network and Information Systems) Bill 2024--26, and sector-specific regimes or requirements).

As part of the project's risk assessment in WP1, such policies/regulations will be monitored for any changes that may impact the overall tool development.
Since the project began, the NCSC has released a migration timeline for PQC which asks that all CNI organisations have a plan by 2028, have all high-priority systems migrated by 2031, and ensure all other systems are migrated by 2035. Our tooling supports those obligations, as our approach will provide an evidenced position on system priority, in addition to the efficiencies outlined in other questions.
It is important to keep up to date with NCSC policy for this project. Cambridge Consultants is one of the NCSC PQC Assured Consultancies and, as such, will receive regular updates about PQC initiatives and guidance. The energy sector partners also have NCSC contacts, and the NCSC will be invited to join our Quantum-Security Advisory Council (Q-SAC).
We will also keep a close eye on PQC migration timelines and policy in other relevant geographies (e.g., EU, USA) to ensure any relevant impacts or learnings can be incorporated.

**Required Changes**
There are no required changes to standards/policy.

**Overcoming Barriers**
There are no barriers; however, we will ensure this position is frequently reviewed as part our overall Project Management risk assessments within WP1.
**Derogations/Exemptions**
The lead partner, NESO, has assessed the project and confirmed no derogations or exemptions now or during the project are/will be required.

## Consumer impact and engagement

**Consumer Needs**
The consumer need addressed by NSiaQF is the need to ensure consistency of energy supply to consumers in as cost-effective a way as possible.
NSiaQF aims to improve the resilience of the energy network by supporting the energy networks in their migration to quantum-

safe cryptography and architectures. Further, it aims to do so in a way that maximises the efficiency and effectiveness of this migration through minimising the impact on the total cost of the assets. This will prevent unnecessary upgrades and embed migration into natural asset lifetimes where possible.

**Benefits to Consumers**
Improving the resilience of the GB energy sector to malicious cyberattacks will reduce the potential for disruption for all consumers.
This is an indirect benefit to all consumers, given the significant cost, social and environmental impact of a disrupted energy supply. However, avoiding supply interruption is also critically important for certain vulnerable groups.
Research carried out by The UK Energy Research Centre in 2021 concluded that unplanned outages disproportionately affect low-income households. This is because they are less likely to have access to alternative heat and cooking options (camping equipment, wood burners) and are also less likely to have adequate insulation for their homes. These factors drive a higher susceptibility to the harms from being cold, which has negative health impacts and increases mortality risk.
Delivering the migration at the best value also delivers direct consumer benefits by ensuring their energy costs are not unduly increased. This could happen if networks have to support the increased investment and maintenance burden of delivering a large-scale, non-prioritised (and, in some cases, unnecessary) replacement of energy network cryptographic assets with quantum-safe equivalents. The NSiaQF tools will therefore protect consumer interests by helping to ensure this isn't necessary.
This benefit also has most impact for lower income households. Those households most likely to benefit from controlling energy costs are those that are already classified as "fuel poor" (an estimated 11% in England, 34% in Scotland, 14% in Wales, and 24% in Northern Ireland according to the UK government report "Fuel Poverty in the UK", 14/03/25).

**Consumer Engagement**
Communicating these benefits will be part of the formal communications plan for the project (Dissemination in WP1).
We plan to ensure that the voice of the consumer is represented during decision-making, and that the benefits of the project will be appropriately communicated to consumers. This will be achieved by inviting a wide range of networks and other organisations to join our Quantum-Security Advisory Council (Q-SAC), for direct consumer-facing representation. We will use NESO's standing relationship with Citizens Advice to this end and will formally invite them to represent consumer views.
We will also create an accessible project video that explains the project to non-experts; this will be made available to interested parties and promoted by the project team.
As part of the project's overall dissemination plan, information regarding the project's aims and final output will be made freely available to the public. A key focus will be how the project outputs support a resilient and cost-effective energy supply for consumers.
These activities will be supplemental to dissemination events at industry forums, and the final show-and-tell session.

- 30-year NPV: £39.3Bn (£578/consumer)

## Value for money

Total cost: £7,211,186
Total contribution: £1,020,186 (14.1%)
Funding requested: £6,191,000 (85.9%)

Cost Breakdown:
Lead Partner: NESO

- Total cost: £2,631,916
- Contribution: £394,787 (15%)
- Funding: £2,237,129 (36% of total)

Partner 1: Cambridge Consultants

- Total cost: £3,254,783
- Contribution: £492,949 (15%)
- Funding: £2,761,834 (45% of total)

Partner 2: University of Edinburgh

- Total cost: £975,072
- Contribution: £97,508 (10%)
- Funding: £ 877,564 (14% of total)

Partner 3: Scottish Power Energy Networks

- Total cost: £202,358
- Contribution: £20,236 (10%)
- Funding: £182,122 (3% of total)

Partner 4: National Gas Transmission

- Total cost: £147,057
- Contribution: £14,706 (10%)
- Funding: £132,351 (2% of total)

**Pre-existing Assets/Facilities**
None.

**Subcontractors, their costs and why they are critical**
Software development subcontractor to be selected before kick-off. Cost (capped estimated based on similar support): £1,015,000
A mini-competition will be run using NESO's D&D Framework to ensure best value-for-money. This route minimises contractual complexity. All suppliers on this framework have already passed all required quality and capability checks.

**Contributions**
All partners are making at least a 10% contribution, funded by:

- NESO, SPEN and NGT through their network innovation budgets.
CC through benefit-in-kind, including discounted project fees.
- UoE by discounting Full Economic Cost (FEC) rates.

NESO and Networks have benchmarked rates approved by Ofgem.
NESO has run a benchmarking exercise to assess CC's rates finding they are competitive with other high-speciality consultancies. CC rates have been reduced for NSiaQF.

**Additional Funding**
No additional funding from other innovation funds has been sought.

**Value-for-money for the Consumer**
In project, value is assured for consumers as discussed above, through:

- Use of discounted rates.
- Subcontracting of development to a subcontractor picked through a competitive NESO framework.
- Benchmarking of commercial partner's rates.
- NESO IP ownership post-project.

More broadly, the UK National Risk Register 2024 estimates the cost of a successful major cyber-attack against the UK national electrical transmission network at ~£50Bn. A quantum-enabled cyberattack at this scale will be possible (and likely, given threat actor intentions) within 10-15 years, based on open-source threat intelligence and published guidance from the NCSC. Consumers would ultimately bear the cost of such an attack through higher energy bills, disruption and wider UK economic/social impacts. As such, networks need to take mitigating action.
NSiaQF tools will therefore enable networks to undertake mitigations in a targeted and well-prioritised way. This will lower mitigation costs and improve their effectiveness, reducing cyberattack risks and delivering VfM for consumers.
In the Baseline scenario, networks rely largely on cybersecurity vendors to provide upgrades to post-quantum security. This requires higher total investment as vendors do not currently have NSiaQF-type decision support tools and would need to rely on manual identification of vulnerabilities. They would charge higher commercial rates, and networks would be more vulnerable for longer.
The alternative 'Rip-and-Replace' strategy assumes networks pre-emptively replace existing assets (ahead of end-of-life) to

ensure security against quantum attacks; this is even more expensive, and also less secure. Compared to NSiaQF tool adoption, both scenarios result in higher costs, higher energy bills for consumers, and greater risk of cyberattack.
To illustrate this, we calculated the total cost of the project and the alternative Rip-and-Replace scenario across the UK's 68m consumers. We also looked at the main benefit: the avoided cost of cyberattacks (vs Baseline). The analysis, which is very conservative as it multiplies cyberattack cost by percentage likelihood, shows clearly that the project delivers exceptional value-for-money for consumers.

**NSiaQF Tool Adoption:**

- Up-front cost of tool development (Beta project): £6.19Mn (£0.09/consumer)
- Total expenditure (from CBA): £849Mn (£12/consumer)
- Avoided cost of cyberattacks: £19.4Bn (£285/consumer)
- 30-year NPV: £83.6Bn (£1,226/consumer)

**Rip and Replace:**
Total expenditure (from CBA): £12.4Bn (£182/consumer)
Avoided cost of cyberattacks: £9.9Bn (£146/consumer)

## Associated Innovation Projects

- (•) Yes (please remember to upload all required documentation)
- ( ) No (please upload your approved ANIP form as an appendix)

## Supporting documents

### File Upload

No documents uploaded

### Documents uploaded where applicable?

☑