**REQUEST FOR QUOTE (RFQ) REF 614 – THE BRIEF**

**PROVISION OF SERVICES FOR: PRIVACY ENHANCING TECHNOLOGIES: ADDRESSING THE USER CONFIDENCE GAP: CERTIFICATIONS, ASSURANCE SCHEMES AND RISK ASSESSMENT TOOLKITS**

1. **Introduction to the Royal Society**

[The Royal Society](https://royalsociety.org) is the national academy for science in the UK. It is a self-governing Fellowship of many of the world’s most distinguished scientists who are elected based on their scientific work. The Society is over 350 years old, and its Fellowship includes names such as Newton, Darwin and Hawking as well as current names such as Dame Uta Frith, Dame Julia Higgins, Sir Venki Ramakrishnan and current Royal Society President, Sir Adrian Smith. The Fellowship embraces the work of discovery scientists and applied scientists and covers the full range of scientific disciplines.

The Society’s fundamental purpose, reflected in its founding Charters of the 1660s, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity. The Society has played a part in some of the most fundamental, significant, and life-changing discoveries in scientific history and Royal Society scientists continue to make outstanding contributions to science in many research areas.

Our priorities are promoting excellence in science; supporting international collaboration; and demonstrating the importance of science to everyone.

1. **Background to the Project**

The Royal Society’s [Data Programme](https://royalsociety.org/topics-policy/open-science-and-data/) is developing policy and promoting debate that helps the UK safely and rapidly realise the growing benefits of data and digital technologies. In 2019, the Royal Society launched the report[*Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*](https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf). One of our activities following from this report is an exploration of the status and role of Privacy Enhancing Technologies (PETs): technologies or conceptual approaches that allow the derivation of useful insights from data without requiring full data access. Some examples include homomorphic encryption, zero knowledge proofs, differential privacy and secure multi-party computation.

The Royal Society has launched a refresher project to update the 2019 report, which will be published in late 2021. This shall include an updated review of PETs applications, legal / regulatory concerns and an illustrative set of use cases. This commissioned review is a foundational piece of our evidence gathering for this project; it will inform our understanding of the regulatory landscape and possible futures with regard to PETs.

1. **Overview of the Services required**

The Society seek to engage a Supplier to provide a review in three parts:

1. a review of certification and assurance of PETs;
2. an overview of certification and assurance practices in cybersecurity since 2000; and
3. a synthesis discussion that draws from both reviews to identify transferrable lessons from the recent history of cybersecurity assurance that may (or may not) apply to PETs.

3.1 Audience

The main audience for this review is the Royal Society policy team, the privacy enhancing technologies working group and expert participants in project workshops.

3.2 Objectives and research questions

The successful Supplier shall undertake preliminary consultations with stakeholders in various sectors (e.g., researchers and innovators in health, energy, security) suggests that PETs would meet vital privacy and security needs, enabling a greater and more beneficial flow of data and information. However, several key ‘sticking points’ have emerged; these include a limited technical knowledge of PETs and concerns around the limitations of PETs in various deployment scenarios.

Without a framework for assessing privacy risk versus utility of data sharing; the user may be reluctant to take on the responsibility of choosing which configuration of PETs would meet their needs. While well-resourced organisations may seek private consultancy with a security expert, the Society believes a broader solution would enable greater uptake of PETs. This could entail, for example., PETs certification and assurance schemes; these would ‘outsource’ an organisation’s PETs risk management exercise to an external regulatory mechanism (akin to those issued to cybersecurity products).

This might also include development of tools that help organisation understand which PETs to deploy in various contexts, including the significance of doing so (e.g., a risk assessment / data management tool kit).

The Society’s primary objective for the provision of this research is to understand user needs: What is needed to foster wider user confidence in deploying PETs? Part of this will involve documenting what exists (data risk vs utility metrics, certification, and assurance schemes with applicability to PETs or relevant cybersecurity examples). The scope of this review should be international but not comprehensive.

The successful Supplier shall provide a review and analysis which shall answer the following questions:

1. What tools exist around evaluating data privacy vs utility, risk assessment and data management with relevance to PETs? What is missing?
2. What PETs certification and assurance schemes exist (nationally / internationally) or might be the subject of current initiatives?
3. What lessons can be drawn from certification and trust marks / kitemarks in cybersecurity (including those agreed at national or international levels) that may be relevant to PETs? Eg, this might include lessons about uptake, public recognition and trust, and user experience.
4. Based on the above reviews, what are the primary drivers for user confidence in PETs or relevant cybersecurity examples?
5. **Outputs**

The successful Supplier shall be responsible for the delivery of a review paper (about 8500 words) addressing the research questions above.

The review paper shall detail the state of existing user tools for evaluating privacy, risk and utility, including PETs certification and assurance schemes in existence (this may include international examples, e.g., relevant NIST activities in the US context). The paper shall also discuss the relevance of certification and trust marks / kitemarks in addressing user needs and trust in cybersecurity, including whether these are agreed on national or international level. Lastly, it shall also highlight evidence of gaps where user needs remain unmet.

The paper shall be reviewed by a steering group of experts from academia, industry, and the public sector.

Revisions / edits will be expected according to a timeline to be agreed with the supplier. References should be inserted in the text and footnoted using Royal Society style (to be provided).

1. **Deliverables**

The successful Supplier shall deliver the following:

1. Findings paper, about 8500 words, with executive summary and
2. Raw data / full sources upon request

5.1 Methodology

This work will primarily involve desk research which may require access to archives or other databases. Please use your proposal to outline your methodology, including your approach to surveying available literature / accessing required information and analysis.

5.2 How will the deliverables be used by the Royal Society?

The Royal Society will use these findings to inform our project work and final refresher report on PETs. The final report text and figures will be designed and published by the Royal Society, with the Royal Society branding. The deliverables will be the property of the Royal Society and will be reusable in print by the author after the first publication by the Royal Society. All contributors will be acknowledged in the final report.

* 1. Project management

An inception meeting and midpoint check-in meetings to be held with Royal Society staff virtually; additional informal updates or clarification may be communicated via regular emails or brief ad hoc meetings via phone / virtual setting.

1. **Timelines**

The successful supplier shall be required to complete the Services by 22 November 2021.

|  |  |
| --- | --- |
| Kick off meeting | w/c 20 September 2021 |
| Midterm check-in to discuss emerging findings | w/c 18 October 2021 |
| Draft report submitted | 8 November 2021 |
| Final report submitted | 22 November 2021 |

1. **Budget**

The Royal Society is a UK registered charity with limited funds, some of which are provided via Central Government grants, and therefore we must report on our expenditure. Suppliers are asked to be mindful of this when proposing their costs and that you are as transparent as possible in your breakdowns.

Any costs for the delivery of the Services stated in this brief that are not identified by Suppliers as part of their pricing shall be expected to be absorbed by Suppliers.

The maximum amount for the Services is up to£6,000 (VAT inclusive).

Please include a detailed breakdown of costs in your proposal using the provided pricing template.

1. **Evaluating proposals**

As part of your proposal, Suppliers are requested to provide statements to the below criteria questions:

| **Criteria No.** | **Criteria Question** | **Weighting** |
| --- | --- | --- |
| 1 | **Experience**: Please provide a statement to your experience of delivering similar Services within the last 3 years.  | 10% |
| 2 | **Understanding the requirements**: Demonstrate your understanding of the brief requirements and objectives | 10% |
| 3 | **Methodology**: Detail how you will achieve the delivery of the Services including a detailed timeline and methodology in consideration of the audience and subject matter in line with this Brief. | 30% |
| 4 | **Proposed Team**: Detail your proposed project team and their experience of delivering similar projects and how you will ensure business continuity for the term of the Services Agreement. Please provide the proposed team members’ CVs. | 20% |
| 5 | **Terms and Conditions**:Please provide a statement as to any possible amendments you may seek to the Society’s standard Terms and Conditions. Please also state any position you have on publishing and acknowledgement of your Services for consideration by the Society. | 0% |
| 6 | **Project Costs**:Pricing and demonstrating value for money by completing the template titled Services Charges providing your proposed costs and rate card charges**.** | 30% |
| **Total** | **100%** |

Please note that the proposed team (criteria no. 4) will be expected to complete the commissioned work if successful. Any personnel changes will be subject to written pre-approval by the Society.

1. **How to respond to this brief**

Please respond by emailing your proposal by 5pm BST on 6 September 2021 including the following June.Brawner@royalsociety.org:

1. Cover note stating your legal name, organisation name, address, phone number, email and UK Company House registration number.
2. Your written proposal addressing all of the Criteria at item 8,
3. Your completed Services Charges template and
4. Your completed Supplier Declaration Form

In the case that any of the above requirements are not completed by the closing date and time, your proposal shall not be eligible for consideration.

Suppliers who can’t not meet the provided timelines are to contact the Society using the below details as soon as possible to discuss.

Attachments included in this Request for Quote:

* Attachment 1 – The Brief
* Attachment 2 – Service Charges template
* Attachment 3 – Terms and Conditions
* Attachment 4 – RFQ Supplier Declaration Form
* Attachment 5 - Supplier Registration Form

Please note that where personal data will be involved, a Data Sharing Agreement may be put in place. This will be discussed with the successful Supplier as part of the Award process.

In your proposal, please declare any professional or personal connections, financial or otherwise, with Royal Society Staff, [Officers](https://royalsociety.org/about-us/committees/council-37/) or members of the [Privacy Enhancing Technologies working group](https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/).

We request any clarification questions be submitted no later than 12pm BST on 2 September 2021. All responses to clarification questions shall be shared with all Suppliers.

Please contact June Brawner (June.Brawner@royalsociety.org) with proposal submissions and questions.

Please complete and email the Supplier Registration Form at Attachment 5 to me so that clarifications can be sent to you.