NSTIx Op-Tech Co-Creation Space

Challenge Form: Long Distance Wi-Fi

Release Date	Proposal Deadline	Expected Start Date	Duration	Indicative Budget
Mon 9th October 2023	Fri 17th November 2023	February 2024	12 weeks	£60k (ex VAT) per solution provider. Higher budgets available for consortia.

Responding to NSTIx OpTech Co-Creation

The National Security Technology and Innovation Exchange (NSTIx) is a government-led science, technology and innovation partnership that enables coherent and agile delivery of innovative national security outcomes through a co-ordinated and systematic approach to research and capability development.

NSTIx has established a government-led network of themed Co-Creation Spaces (CCS). The CCS' combine the respective power of specialist public and private sector partners in research, capability development and end user requirements. This supports the development of effective, user-driven technology at pace in areas that are critical to national security. For more information, please see the 'NSTIx Leaflet' in digital form (https://www.gov.uk/government/publications/nstix-information-leaflet).

Op Tech Co-Creation (OCCS) has engaged with a network of key Community Collaborators, to accelerate and leverage access to their existing networks of industry and academic Solution Providers.

By responding to this Challenge (details provided in 'Solution Provider Proposals – 'our ask' section) and participating in Co-Creation there is an exciting opportunity for collaboration between National Security, Community Collaborators and Solution Providers.

What is the current state for this Challenge?

The invention of Wi-Fi has clearly had an impact on society with its ubiquity taken for granted. There are ongoing issues for useability in certain niche scenarios. A Wi-Fi router range will vary depending on the environment but could be from just a few metres to tens of metres. To extend this range, extenders and additional Wi-Fi Access Points (AP's) are typically used. This becomes complex in congested Radio-Frequency (RF) environments like the ones found in dense urban environments in particular at the 2.4 GHz and 5 GHz band, resulting in interference and postponing of transmission (Ruirong Chen *et al.*, SenSys 2022) though Wi-Fi 7 goes some way to resolve this.

What is the gap?

There is a client-side gap connecting to a Wi-Fi AP from a significant distance away, potentially hundreds of metres, up to a kilometre, particularly in congested RF environments.

National Security personnel who operate globally use internet connected equipment in scenarios where it is not desirable or possible to connect to a third party Wi-Fi AP or cellular provider.

Examples include countries where there are concerns about the privacy and cyber security of third-party Wi-Fi or cellular connections and the only option is to connect to their own secure and trusted Wi-Fi AP. In addition, disaster areas where there is a reduced internet service provided due to local infrastructure damage and the only desired option is to connect to Wi-Fi Aps or cellular base stations that are out of current range.

In these scenarios, it is typical for rapid mobile deployment teams to be on the move and out of current range from any UK estate with a secure WI-FI AP or a working internet connection disaster area. The mobile teams may only remain on location for a matter of hours or days, so it is unlikely they will have capacity to install additional internet infrastructure. It may also not be feasible to alter the Wi-Fi AP they are attempting to connect to, such as increasing power.
This challenge is to address a client-side solution which would give access to a Wi-Fi AP from several hundreds meters, up to a kilometre, in dense urban environments with congested RF signals.

This Challenge

We would like to develop a system to receive a Wi-Fi signal from at least several hundred metres, up to a kilometre, in dense urban environments with congested RF signals. This would connect to a client device (i.e. Laptop, tablet, Mobile Phone) to supply a stable Wi-Fi connection.

There can be no alterations to the Wi-Fi AP, conversely there are no operating restrictions on the client-side. Size is of no issue, although consideration should be given to mobile deployment teams who travel in SUV's or small vans. Power is also of no issue at this stage and will be considered as the solution develops.

We are keen to hear from a spectrum of ideas, from TRL1-9, basic research, feasibility, up to off-the-shelf product development. To help shape this challenge, here is a non-exhaustive list of ideas that you may consider:

- Horizon scanning solutions using expertise and knowledge of commercial offerings.
- Environmental RF modelling.
- RF Interference cancellation to signal boost, which could be AI/ML enabled.
- RF Repeaters.
- Beam Forming.
- Innovative Antennas.

What we don't want

We are open to all ideas at this stage.

Follow-on Project

If this challenge cannot be solved in 12 weeks and the initial solution demonstrates feasible concepts, and the OCCS teams agree, follow-on funding is likely.

Solution Provider Proposals – 'our ask'

This Challenge is open to sole innovators and to organisations of all types and sizes. This includes UK registered businesses of any size, Universities, and research and technology organisations.
Consortiums are encouraged where a sole lead organisation contracts with the Authority & flows the terms, conditions, IP & payments, to the consortium members.

The Authority will evaluate tenders in accordance with the procurement principles of transparency, equal opportunity and non-discrimination & evaluation criteria provided. The Authority reserve the right to make the final decisions as to which proposals are taken forward to apply for funding in the competition.

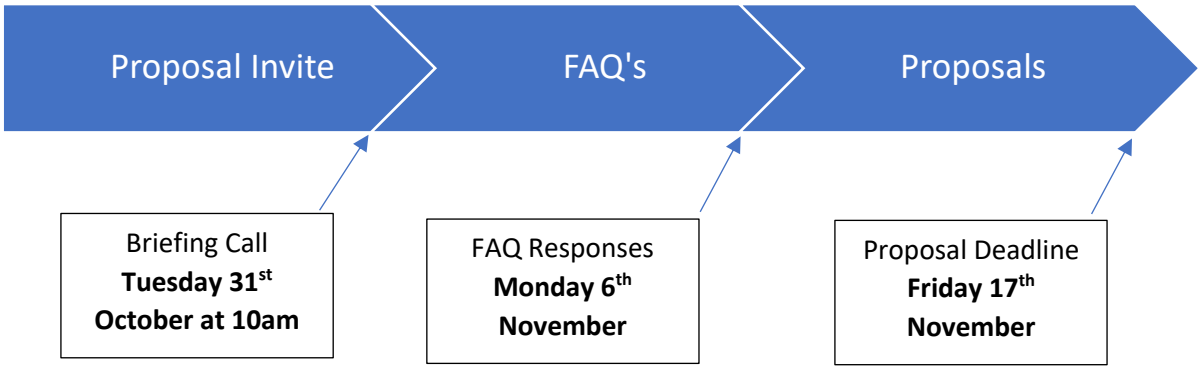
Proposals are requested by the deadline of **Friday 17th November 2023.** An agile approach over the **12-week** period is preferred, with sprints designed to work with the National Security community to iteratively define the solution. We have an indicative budget of **£60k** for a single solution provider, budget increases will be considered for consortiums.

Evaluation criteria

Proposals will be scored 1 – 5 on the following criteria:

- Timescale – will the proposal deliver a Minimum Viable Product within the time period defined within this Challenge Form?
- Does the proposal fit within the Challenge scope, taking into consideration cost and benefits?
- Is the organisation / delivery team credible in this technical area?
- Is the technical solution credible?
- Will the proposal deliver a full or partial solution? Has the proposal identified collaborators if a partial solution or is willing to work collaboratively with others?
- Is it innovative?

Next Steps



Confidentiality: All proposals will be subject to commercial confidentiality and a maximum protective marking of OFFICIAL. Please do not submit any materials above this classification.

Briefing Call: All parties will be invited to an open Briefing Call via MS Teams on **Tuesday 31st October at 10am**, where members of the OCCS Challenge Team will be available to provide additional context and information on this Challenge, and where attendees can ask clarification questions.

Please click here to access the call

Failure to attend the Briefing Call or pre-competition events does not exclude solution providers from submitting a proposal by the deadline stated below.

Frequently Asked Questions – responses (FAQ): All enquiries from the Briefing Call will be collated, and responses sent to all parties in an FAQ document by **Monday 6th November**.

Pricing: Solution providers are invited to submit **Fixed Price** proposals for the **12-week** engagement. When preparing pricing please provide pricing against 3 monthly payment points in line with the sprint-profile of your project.

Deadline: The deadline for proposals to be submitted is close of business on **Friday 17th November.**

Submissions: Please send your proposals via the Community Collaborator you found this Challenge, alternatively you can send it directly to cocreation@hmgcc.gov.uk, but please note where you first heard of this Challenge. Ensure you include the title of the Challenge '**Wi-Fi access Points'** in your submission.

Format: Final responses for this Challenge can be provided in any format, they will be assessed on the quality of the information as per the Evaluation Criteria. Some Community Collaborators only allow a certain word count in their submission forms, if you need to provide further information, please include attachments.

Selection and notification of finalists: The OCCS Challenge Team aims to select a shortlist of successful proposals by **week commencing Monday 27th November** and invited to a pitch day.

Pitch day: The OCCS Challenge Team pitch day will be on **Thursday 7th December 2023**. An option to attend face to face or online will be made.

Feedback: All applicants will be provided with written feedback via the Community Collaborator once both technical and commercial assessments have been concluded. We will endeavour to provide feedback within 2 weeks of the competition deadline.

Commercial Engagement: The OCCS challenge team will select Solution Providers for this Challenge on the technical and commercial merit of the proposal received, commercial contracts and funding will be engaged through Cranfield University. Intellectual Property deliverables will be engaged with the OCCS under the terms attached.

Project start date: The target start date of contracted solution providers is **the beginning of February 2024**.

Commercial Considerations – Regardless of the Commercial Route Selected the following terms apply:

Please note that by submitting a proposal in response to this challenge you are agreeing to the terms and conditions of contract as issued and are thereby making a formal offer of contract, from which the Authority shall have the right to accept in part or in full should your proposal be deemed acceptable.

#	Category	Consideration
1	IP	Intellectual Property (IP) will be managed in accordance with the attached Terms & Conditions.
2	NDA	It is the responsibility of the Community Collaborator to propagate and adhere to the agreed Non-Disclosure Agreements (NDAs).
3	IT Systems	The Community Collaborator and/or Solution Provider IT system will be used as the collaboration platform for developing solutions to this challenge (including for example MS Teams, SharePoint, plus any required development and test

		environments). Systems must be capable of holding documents marked at OFFICIAL.
4	Data	All data will be managed in accordance with UK Data Protection legislation. This includes commercial & project documentation, and any data utilised in developing, testing and implementing the solution for this challenge.
5	Scope	Solution providers for this challenge may be from the UK or 5EYES geographies. Other geographies will be considered on a case-by-case basis.
6	Clearance	All work will be classified at no higher than OFFICIAL. It is desirable for resources working on the project from Community Member organisations to have BPSS or SC (or equivalent) clearance, however this is not essential at this stage. Collaborators are asked to please state the clearance levels of their proposed Project Team within their submitted proposals.