NSTIx Op-Tech Co-Creation Space

Challenge Form: Mapping industrial assets in a complex environment

Release date to public	Proposal Deadline	Expected Start Date	Duration	Indicative Budget
Mon 11th September 2023	Fri 20th October 2023	4 weeks after proposal accepted	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?

National Security have a duty to advise and play a role in protecting National Infrastructure (NI), such as the energy and water networks. For NI organisations to effectively apply security controls protecting from external threats, such as a cyber-attack, knowing what assets are within the network is fundamental. Taking the energy network as an example, the complexity of entire system is vast

- There are many large assets such as power stations, gas pipelines, interconnectors, storage facilities and substations.
- These are broken down into many different smaller assets such as computer control systems and metering, modems, sensor nodes, transceivers, data centres, switches, and firewalls.
- These are run by many different operators such as energy generation organisations, aggregators, distribution network operators, and transmission network operators.
- These have unique challenges such as proprietary protocols, varied wired and wireless communication mediums and geographic distribution.
- Active scanning is often discouraged in the Operational Technology (OT) space, as it is perceived to have potential to slow or disrupt the functionality of connected systems.

All of this combined, makes asset management and discovery vastly complex and results in a high barrier to entry for a new organisation into this supply chain.

What is the gap?

Current solutions for OT asset discovery are often expensive and require a large amount of network changes to install, so they are typically limited to large, established companies. They typically use passive identification techniques, use a lot of sensors, and often change the architecture which develop delays in the system. Aggregated data is then forwarded from routers, switches, firewalls, as well as the OT data historians.

There is a need to lower the bar to develop more affordable solutions to map industrial assets, and this Challenge seeks to encourage small to medium organisations to develop technology and enter the market.

Asset mapping tools need to achieve the best coverage possible, whilst minimising the impact on the assessed network. Areas to explore include how black spots in data collected can be used to predict the presence of undetected assets. This could be identified traffic to a device that is known to be a serial to IP convertor, or a Supervisory Control and Data Acquisition (SCADA) gateway. These areas need to be highlighted in the tools reporting, to show areas that current asset inventories will not provide visibility of, including where serial or RF data flows could be present.

This Challenge

This Challenge will last for 12 weeks with an indicative budget of £60k (ex VAT) per solution provider, with higher budgets available for consortiums. The focus of this Challenge is to encourage small to medium sized organisations to enter the OT cyber-security market space, by funding highly innovative developments of asset mapping systems to map conventional IT hardware as well as OT components such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Sensors/Actuators, Serial Convertors, SCADA Gateways and more, a to a target TRL 4 concept demonstrator(s).

To steer the Challenge developments:

- The system must be able to rapidly analyse an arbitrary connected system with any combination of hardware and software.
- The developed system must allow the target system to continue functioning as normal without any degradation of performance.
- The developed system must identify individual system components in varying environments.
- The developed solution must identify system to system connections and data flows.
- The developed system must ensure results are accurate and provide a high level of coverage across the target estate, this will need to be demonstrated against baselines.
- The developed system should aim to identify and report on data blackspots where traffic is being sent to protocol convertors or gateway devices, out of bounds of the assessed network.
- Passive solutions are preferred.

Stretch targets:

- The developed system should aim to look for system configuration issues or system level vulnerabilities (i.e. outdated firmware)
- The developed system could utilise Artificial Intelligence to assist with the discovery of assets however, this must not introduce false positives and results from this technique should be tagged.

- Visualisation solutions such as VR/AR options.
- The developed system could provide recommended corrective intervention actions in priority order.
- The developed system could aim to understand assessment of system security and compliance threats e.g., using the Microsoft STRIDE framework (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege).
- The system could be developed with consideration to the potential legal, physical, and cognitive risks (probability and impact) to the system, its users, or the wider connected system-of-systems.

Demonstrator(s) must be documented and final report submitted.

What we don't want

- Expensive and manual approaches.
- Established companies to develop high-TRL technology.
- A paper-based only study.

Follow-on project

If this initial project shows the concept to be feasible, and the OCCS team agree, a funded follow-on project will be likely. There may also be the potential to offer alternative benefits such as invitations to National Security start-up accelerator programmes.

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.

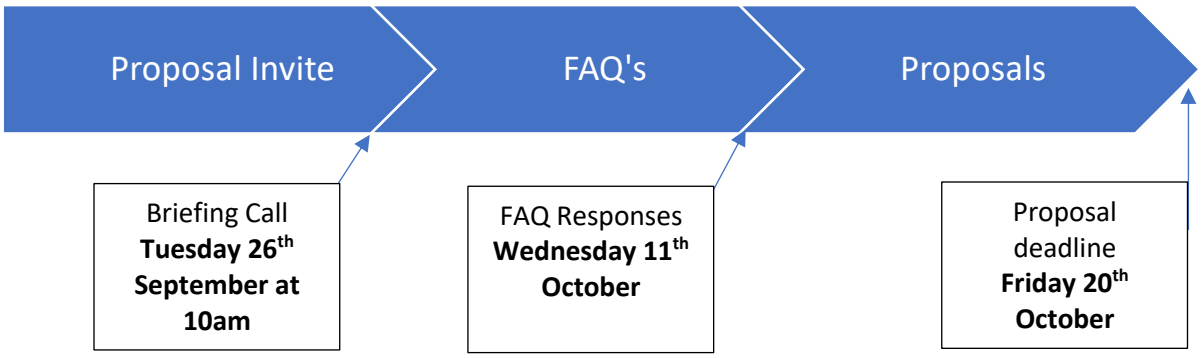
Proposals are requested by the deadline of **Friday 20th October 2023.** An agile approach over the **12 week** period is preferred, with sprints designed to work with the National Security community to iteratively define the solution. We have an indicative budget of **£60k** for a single solution provider, 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.

Technology Readiness Level (TRL): A cross-section of TRLs 1 – 4 will be considered for this Challenge.

Briefing Call: All parties will be invited to an open Briefing Call via MS Teams on **Tuesday 26th September 2023 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 see the link below:
Click here to join the meeting

Meeting ID: 341 463 187 75
Passcode: WGZfgT

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 **Wednesday 11th October 2023**.

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 20th October 2023.**

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 do note where you first heard of this Challenge. Ensure you include the title of the Challenge '**Mapping industrial assets in a complex environment'** 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 **Monday 30th October 2023** and invited to a pitch day.

Pitch day: The OCCS Challenge Team pitch day will be on **Thursday 9th November 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 project start date of contracted solution providers is **Monday 11th December 2023**.

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.

*Onboarding of a company onto our commercial Terms & Conditions can take up to an additional 4 weeks.