HMGCC
Co-Creation

Challenge: Rapidly deployed tech to track intruders

Summary of the challenge

The UK government requires temporary use spaces to be secured ensuring they haven’t been entered and compromised whilst left physically unattended. Intruder monitoring systems that can be easily and quickly deployed by non-technical staff are being sought in the latest challenge released by HMGCC Co-Creation.

The team is keen to hear from experts in technology which can rapidly find and monitor intruders – with a particular focus on using high-tech sensors, portable power and encrypted communication.

Organisations are being asked to apply develop and demonstrate technology to meet this challenge over a 12-week period, HMGCC Co-Creation will provide funding for time, materials, overheads and other indirect expenses.

Key information

Budget per single organisation, up to	**£60,000**
Project duration	**12 weeks**
Competition opens	**Monday 18 November 2024**
Competition closes	**Thursday 19 December 2024 at 5:00pm**

Context of the challenge

The UK government operates permanent and temporary facilities globally in various environments. Once a new location has been selected, unauthorised access is prevented by various means prior to and during occupation of that space. However, it is not always possible to deploy permanent intruder monitoring systems in some situations.

The gap

A leave behind and standalone intruder detection system that can be rapidly deployed by non-technical staff is required. This is a chance to explore using high-tech sensors which may not be available in standard long-standing systems, but which could be deployed into these types of alarm.

Example use case

A delegation of government officials is expected to occupy a building in an on overseas city while attending a trade and business investment seminar. Sensitive conversations and activities will need to take place in the building, and it is important these are protected.

Once the building has been selected, it is important that it is secured as soon possible ensuring it hasn't been compromised prior to government officials occupying this space. The officials may also need to be away travelling for some of the time when in the country, so they must have the confidence that, even if the building is left unoccupied, there is no chance that unauthorised intrusion can have taken place. The temporary building will already have been furnished with a level of protection meeting certain UK government security standards.

This particular overseas location does not have a reliable power infrastructure, so power outages can take place. Although the building has a back-up system, this will only provide power for a limited period. Prolonged outages could mean that crucial systems, such as an intruder monitoring system, could be interrupted.

Project scope

The output of the 12-week project should focus on demonstrating technology that shows potential for follow-on projects. This is open to Technology Readiness Levels from 4 – 7, and could focus on different parts of the challenge, such as:

1. High-tech sensors for intruder monitoring.
2. Full system development, considering ease of use (e.g., sensors easy to install, GUI, etc.).
3. Encrypted communication to ensure that information captured from the sensors has a low probability of interception.

Mandatory targets for a solution are listed below. This doesn't necessarily need to be solved during the 12-week project, but a clear path to provide a solution for this must be considered.

- Must sense human presence in an environment.
- Must be power efficient and be able to run for extended periods of time without mains power (although backup power doesn't have to part of the solution).
- Must demonstrate that it is (or could be) useable and deployable to non-technical personnel.
- Must be scalable to be deployed from a single room up to a large-scale facility.
- Must offer remote monitoring in real time.
- Must be usable world-wide.
- A full system must have an API to allow integration into existing monitoring solutions.
- Must have anti-tamper and anti-jamming capability.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

- The system must comply with International Air Transport Association (IATA) dangerous goods regulations (such as lithium battery regulations used as backup power options) to enable transport on regular commercial flights.

Targets that should or could be met, and further considerations:

- The communication from the sensor/processor to the user should be encrypted.
- It could use low-power processing methods such as edge artificial intelligence reducing power consumption.
- It could have different modes of operation, for example if a system uses multiple sensors, then power saving modes could be initiated to turn off certain sensors.
- During development, an alarm system does not need to conform to BS-EN50131, but this should be considered for future phases of work.
- The solution could sense if a perimeter has been compromised by non-human presence outside the specified boundary (e.g. a drone).
- The system should be small enough to be easily carried by a person, for example aircraft cabin bag size.
- The system should be able to securely log data locally, for instances when the remote monitoring link is unavailable.
- The system should be able to push notifications to end users.
- The system could have multi-sensor verification.

Please note:

This challenge will not consider solutions using basic sensors such as passive infrared (PIR) and cameras.

Dates

Competition opens	Monday 18 November 2024
Online Briefing Call	Thursday 28 November 2024 at 10:00am
Clarifying questions published	Thursday 5 December 2024
Competition closes	Thursday 19 December 2024 at 5:00pm
Applicant notified	Thursday 9 January 2025
Pitch day in Milton Keynes	Thursday 16 January 2025

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

Pitch Day outcome	Friday 17 January 2025
Commercial onboarding begins*	Monday 20 January 2025 at 3:00pm
Target project kick-off	Monday 3 February 2025

**Please note, the successful solution provider will be expected to have availability for a 1-hour onboarding call via MS Teams on the date and time specified to begin the onboarding/contractual process.*

Eligibility

This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes. There is no requirement for security clearances.

Solution providers or direct collaboration from countries listed by the UK government under trade sanctions and/or arms embargoes, are not eligible for HMGCC Co-Creation challenges.

How we evaluate

All proposals, regardless of the application route, will be assessed by the HMGCC Co-Creation team. Proposals will be scored 1–5 on the following criteria:

Scope	Does the proposal fit within the challenge scope, taking into consideration cost and benefit?
Innovation	Is the technical solution credible, will it create new knowledge and IP, or use existing IP?
Deliverables	Will the proposal deliver a full or partial solution, if a partial solution, are there collaborations identified?
Timescale	Will the proposal deliver a minimum viable product within the project duration?
Budget	Are the project finances within the competition scope?
Team	Are the organisation / delivery team credible in this technical area?

Invitation to present

Successful applicants will be invited to a pitch day, giving them a chance to meet the HMGCC Co-Creation team and pitch the proposal during a 20 minute presentation, followed by questions.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

After the pitch day, a final funding decision will be made. For unsuccessful applicants, feedback will be given in a timely manner.

Clarifying questions

Clarifying questions or general requests for assistance can be submitted directly to cocreation@hmgcc.gov.uk, please also copy to Co-Creation@dstl.gov.uk, prior to the cut-off date. These clarifying questions may be technical, procedural, or commercial in subject, or anything else where assistance is required. Please note that answered questions will be published to facilitate a fair and open competition.

Routes to apply

HMGCC Co-Creation is working with a multiple and diverse set of community collaborators to broadcast and host challenges. Please follow this link for the full list of community collaborators.

If possible, please submit applications via a community collaborator.

If the community collaborator does not host an application route, please send applications directly to cocreation@hmgcc.gov.uk and also Co-Creation@dstl.gov.uk, including the challenge title with a note of the community collaborator where this challenge was first viewed.

All information you provide to us as part of your proposal, whether submitted directly or via a collaborator platform, will be handled in confidence.

How to apply

Applications **must** be no more than six pages or six slides in length. HMGCC Co-Creation reserve the right to stop reading after 6 pages if this limit is breached. The page/slide limit excludes title pages, references, personnel CVs and organisational profiles.

There is no prescribed application format, however, please ensure your application includes the following:

Applicant details	Contact name, organisation details and registration number.
Scope	Describe how the project aligns to the challenge scope.
Innovation	Describe the innovation and technology intended to be delivered in the project, along with new IP that will be generated or existing IP that can be used.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

Deliverables	Describe the project outcomes and their impacts.
Timescale	Detail how a minimum viable product will be achieved within the project duration.
Budget	Provide project finances against deliverables within the project duration.
Team	Key personnel CVs and expertise, organisational profile if applicable.

Co-Creation terms and conditions

Proposals must be compliant with the HMGCC Co-Creation terms and conditions; by submitting your proposal you are confirming your organisation's unqualified acceptance of Co-Creation terms and conditions.

Commercial contracts and funding of successful applications will be engaged via our commercial collaborator, Cranfield University.

HMGCC Co-Creation supporting information

HMGCC works with the national security community, UK government, academia, private sector partners and international allies to bring engineering ingenuity to the national security mission, creating tools and technologies that drive us ahead and help to protect the nation.

HMGCC Co-Creation is a partnership between HMGCC and Dstl (Defence Science and Technology Laboratory), created to deliver a new, bold and innovative way of working with the wider UK science and technology community. We bring together the best in class across industry, academia, and government, to work collaboratively on national security engineering challenges and accelerate innovation.

HMGCC Co-Creation is part of the NSTIx Co-Creation network, which enables the UK government national security community to collaborate on science, technology and innovation activities and to deliver these in partnership with a more diverse set of contributors for greater shared impact and pace.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by utilising in-house delivery managers working Agile by default. This process will involve access to HMGCC Co-Creation's technical expertise and facilities to bring a product to market more effectively than traditional customer-supplier relationships.

FAQs

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

1. **Who owns the intellectual property?**

As per the HMGCC Co-Creation terms and conditions, project IP shall belong exclusively to the solution provider, granting the Authority a non-exclusive, royalty free licence.

2. **Who are the end customers?**

National security users. This is a wide range of different UK government departments which will vary from challenge to challenge. This is a modest market and so we would encourage solution providers to consider dual use and commercial exploitation.

3. **What funding is eligible?**

This is not grant funding, so HMGCC Co-Creation funds all time, materials, overheads and indirect costs.

4. **How many projects are funded for each challenge?**

On average we fund two solution providers per challenge, but it does come down to the merit and strength of the received proposals.

5. **Do you expect to get a full product by the end of the funding?**

It changes from challenge to challenge, but it's unlikely. We typically see this initial funding as a feasibility or prototyping activity.

6. **Is there the possibility for follow-on funding beyond project timescale?**

Yes it is possible, if the solution delivered by the end of the project is judged by the HMGCC Co-Creation team as feasible, viable and desirable, then phase 2 funding may be made available.

7. **Can we collaborate with other organisations to form a consortium?**

Yes, this is permitted.

8. **I can't attend the online briefing event, can I still access this?**

If any additional information comes up during the Briefing Call this will be captured and made available via the HMGCC Co-Creation community collaborators.

9. **What are the vetting / security clearances requirement to work with HMGCC Co-Creation?**

Our preference is all work to be conducted at OFFICIAL. As default there is no vetting or security clearance requirement prior to contract award, we may however ask during the course of the project that personnel undertaking work complete BPSS vetting or equivalent, which HMGCC Co-Creation will sponsor.

10. **We think we have already solved this challenge, can we still apply?**

That would be welcomed. If your product fits our needs, then we would like to hear.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.

11. Can you explain the Technology Readiness Level (TRL)?

Please see the UKRI definition for further detail.

12. Can I source components from the list of restricted countries, e.g. electronic components?

Yes, that is acceptable under phase 1 - feasibility, as long as it doesn't break UK government trade restrictions and/or arms embargoes.

Further considerations

Solution providers should also consider their business development and supply chains are in-line with the National Security and Investment Act and the National Protective Security Authority's (NPSA) and National Cyber Security Centre's (NCSC) Trusted Research and Secure Innovation guidance. NPSA and NCSC's Secure Innovation Action Plan provides businesses with bespoke guidance on how to protect their business from security threats, and NPSA and NCSC's Core Security Measures for Early-Stage Technology Businesses provides a list of suggested protective security measures aimed at helping early-stage technology businesses protect their intellectual property, information, and data.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure requests to the originating department.