HMGCC Co-Creation

Challenge: Cutting eavesdropping risks using AI

Summary of the challenge

UK government offices often host sensitive conversations, and it is important to ensure that these are not under threat from accidental or nefarious eavesdropping attempts. These risks are continually assessed due to the high pace of change in technology.

In its latest challenge, HMGCC Co-Creation wants to hear from organisations developing artificial intelligence / machine learning techniques that provide advanced noise cancellation to help us understand what is now possible and to test in a government office scenario.

Organisations are being asked to apply if, over a 12-week period, they can develop and demonstrate technology to meet this challenge, 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	**Thursday 10 October 2024**
Competition closes	**Thursday 7 November 2024**

Context of the challenge

Government offices are often found in multi-occupancy buildings and open plan offices. All offices are designed to National Protective Security Agency specifications, to ensure a standard in physical and cyber protection. But there is more to learn.

Understanding risk in this type of working environment is an important function. If there is an opportunity for eavesdropping, either accidentally or by a nefarious party, we would like to understand how challenging it would be to cancel out the irrelevant ambient noise to focus in on the conversation of significance.

The latest challenge launched by HMGCC Co-Creation sets out to understand the threat of third parties using artificial intelligence (AI) / machine learning (ML) to cancel out randomised and unwanted noise.

The gap

Within office environments, there is a general noise from heating, ventilation, air conditioning systems (HVAC), desk fans, doors closing and background conversations. All of this constitutes random noise generation.

What is already known about how to cancel this noise out? Digital signal processing with adaptive filtering is well known. We want to know more about the threat of cutting-edge methods to increase signal to noise ratios, used to focus on specific conversations.

There has been a rapid rise in recent years of AI and ML adoption in most sectors. There has also been interest and advanced research into using deep learning and neural networks to provide real-time noise cancellation. HMGCC Co-Creation is now seeking to better understand the threat through testing advanced noise cancellation capabilities.

Example use case

Government employee Sam is having a private call in an office booth. The booth is open but designed to dampen leaking sound to the external office. For other office users standing close by there is limited sound leakage, so Sam's conversation can stay private.

The outer area of the office is open plan and there are various online calls happening, as well as general office noise.

Shauna is a few metres away from Sam, using her phone. The phone is picking up all the audio in the room but with the general office noise, Sam's conversation is unlikely to be recorded to an intelligible level, whether the audio was picked up accidentally (over a phone call) or nefariously (by taking an active recording).

If audio was downloaded from Shauna’s phone, there are existing software packages that could be used to remove background noise. However, the following points should be considered:

- Software packages are typically focused on the commercial market, such as podcasting, music recording, and online calls, where there is a controlled and predictable environment of microphone placement and high signal to noise ratio.

- Software packages are unlikely to filter between other less sensitive conversations in the office and focus on Sam's private conversation.
- Shauna's microphone is dynamic, she may decide to sit in a different area or move about, all while still picking up audio. Shauna's phone contains a single microphone, not an array of microphones.

In this scenario, it is highly unlikely that Sam's conversation could be intelligibly intercepted from Shauna's phone even with modern post processing techniques. But could advances in AI / ML audio processing pose more risks?

Project scope

HMGCC Co-Creation would like to team up with organisations developing AI / ML noise cancellation that could be used in busy office environments to focus in on specific conversations. This is to enable better understandings of future threats through demonstration.

Applications to this challenge should already be developed to a mid-Technology Readiness Level (TRL). During this project the HMGCC Co-Creation team can provide limited test data and, at the close of the project, intend to take the developed software and test within a representative lab environment.

The deliverable at the end of a 12-week project should be test results, a report, software that HMGCC Co-Creation can further test and a pathway to further development if more funding is made available.

Considerations for a proposal:

- AI / ML algorithm tested against random (rather than pseudo-random) noise generation.
- Test against non-repetitive speech.
- To understand the theoretical limits of signal to noise ratio in decibels (dB), where the AI / ML code stops working effectively.
- The system would be expected to deliver intelligible speech at very low signal to noise ratios.
- The report and testing should outline signal-to-noise ratio improvement (in dB) across a range of input signal to noise ratios.
- Due to project duration, it is unlikely that there is time for significant model training.
- The software should have the facility to be trained by the end user to optimise performance with their own noise source.

The proposed solution should not be:

- Based solely upon adaptive filtering.
- Horizon scanning.

Dates

Competition opens	Thursday 10 October 2024
Deadline for clarifying questions	Thursday 24 October 2024
Clarifying questions published	Tuesday 29 October 2024
Competition closes	Thursday 7 November 2024 at 5pm
Applicant notified	Wednesday 20 November 2024
Pitch day in Milton Keynes	Thursday 28 November 2024
Target project kick-off	Monday 6 January 2025

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.

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 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 are working with a multiple and diverse set of community collaborators to broadcast and host our 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, 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. The page/slide limit excludes 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.
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.

HMGCC 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 HMGCC 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

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 include a wide range of different UK government departments which varies 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, 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, multi-disciplinary consortiums are encouraged. But please note on this challenge there are no higher budgets for consortiums.

8. **Do we need security clearances to work with HMGCC Co-Creation?**

Our preference is work to be conducted at OFFICIAL, we may however, request the project team undertake BPSS checks or equivalent.

9. **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 about it.

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

Please see the UKRI definition for further detail.

11. **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.