HMGCC
Co-Creation

Personal electronics detector to stop data leak risk

Summary of the challenge

Detectors to spot hidden phones, smart watches or other electronic devices are sought in the latest challenge launched by HMGCC Co-Creation.

To prevent sensitive data being leaked, high classification government areas do not allow personal electronic devices (PEDs) such as phones.

In this challenge, we want to hear from organisations which have or could develop a PED detector to alert people to the presence of a banned device.

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 ex. VAT**
Project duration	**12 weeks**
Competition opens	**Monday 12 May 2025**
Competition closes	**Thursday 12 June 2025 at 5:00pm**

Context of the challenge

UK government, international allies and strategic partners, have facilities with high classification areas, with an increased level of security in place. In these locations, it is vital to ensure no secret recording with prohibited devices like phones or smartwatches is allowed to happen.

The gap

Good security culture and vigilance goes a long way to solve this problem, but a technical solution is required to detect and alarm, with the presence of a PED. The solution will operate in a high classification area, so must not inadvertently record sensitive information itself. The solution should also be adaptable so when new RF bands are used in commercially available PEDs, it can still detect their presence.

Example use case

Jax works in a government building, typically in a low classification space where she is allowed PEDs. But sometimes she has to access a higher classification area where they are not allowed. On one occasion, when Jax is in a hurry, she rushes to a meeting in the higher classification space but forgets she is wearing her smartwatch. This is a genuine mistake, but it could have the unintended consequence of recording sensitive information.

However, the PED detector identifies the presence of an RF signature before the meeting even starts. Responding to this alert, all attendees check, and Jax realises she is wearing her smartwatch. Although embarrassing, this early detection is easier to deal with than the watch being found after the meeting.

Project scope

In this 12-week project, applicants should aim to deliver a demonstration to the sponsors alongside a report. This is open to Technology Readiness Levels (TRL) from 4 – 9. It is recommended that proposals label both the existing TRL and the TRL expected by the end of 12 weeks. Essential, desirable and stretch targets are listed below.

Essential requirements:

- Must be relatively small and unobtrusive.
- Alarm when a PED has been detected with a high degree of confidence.
- Should detect all type of PEDs.
- Consider capturing RF energy only to ensure the solution is not reliant on frequency or protocol detection that can change over time.
- Strictly passive monitoring.
- High degree of confidence when alarm happens. Consider Ability to baseline RF traffic or self-learn about the environment. A detector that alarms even when no prohibited PEDs are in the area could result in users ignoring it.
- Intended to be used globally. Allow privileged users the ability to program the unit.
- Device alarm should consist of both audible and visual keys.

Desirable:

- Battery backup.
- 500MHz – 8GHz frequency monitoring range.
- Easy to operate for a user.
- For wide adoption it must be relatively low cost. Consider what final costings per fully productionised unit may be.
- Include notifications for the occupants of the room
- Display the frequency or signal strength and band that triggered the alarm along with the network provider being used (if a cellular connection)

The environment and constraints:

- PED detector will be static in a meeting room, so can use mains.
- The PED detector will operate in an area without regular access to the internet.
- Wi-fi and other baseline RF signals may be present in some spaces, but necessarily available for the PED detector.

Not required:

- Horizon scanning only.
- Wireless intrusion detection system.
- RF protocol detector.

Dates

Competition opens	Monday 12 May 2025
Deadline for clarifying questions	Tuesday 27 May 2025 at 10am
Clarifying questions published	Tuesday 3 June 2025
Competition closes	Thursday 12 June 2025 at 5pm
Applicant notified	Tuesday 24 June 2025

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

Pitch day in Milton Keynes	Tuesday 1 July 2025
Pitch Day outcome	Monday 7 July 2025
Commercial onboarding begins*	Friday 11 July 2025
Target project kick-off	Tuesday 5 August 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?

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

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 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 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.
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 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?**

   There will be one solution provider for this 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, however no extra funding will be available for this challenge so the consortium would need to operate within the advertised budget

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

   If a briefing event is held, which varies challenge to challenge, then yes. Either the recording or the transcript will be made available to view e after it has been broadcasted. This will be made available via the HMGCC Co-Creation community collaborators.

This information may be exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to the originating department.

9. **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.

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 about it.

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.