Challenge: Dashcam Interruption

Summary of the challenge

Organisations and solution providers can apply for funding to demonstrate the feasibility of preventing a dashcam recording at a pinch-point location.

OpTech Co-Creation will provide all funding for time, material, overheads and other indirect expenses. It is the aim to fund two projects per challenge although there is no determined total budget amount, as the strength of received proposals will be a factor. Multi-organisation consortia are encouraged to apply where appropriate.

Key information

Budget per single organisation, up to	**£60,000**
Budget per consortium, up to	**£120,000**
Project duration	**12 weeks**
Competition opens	**Monday 20 November 2023**
Competition closes	**Thursday 11 January 2024**

Context of the challenge

Numerous secure government facilities across the UK require a form of approved identification permitting entrance. These security measures effect both foot traffic and vehicle access to secure car parks. Unauthorised cameras or other recording equipment are typically not permitted on-site, and with the proliferation of dashboard cameras (dashcams) in vehicles adds an additional element of security concern, as they may inadvertently record facilities, road layouts and personnel information. After the incident, the vehicle may leave the car park inadvertently carrying uncontrolled classified information.

The gap

Policies exist to minimise the use of dashcams within secure government facilities, but it is unlikely that this will prevent all cases from inadvertent recordings by staff or visitors, and even more so would not prevent nefarious clandestine recordings. Further to this, some modern vehicles have integrated cameras built-in which can only be disabled through a software “toggle”, which the vehicle owner may not even be aware of. These are likely to become more prevalent in future, and possibly even “standard fit”. This is coupled with a high throughput of vehicles, potentially hundreds in some facilities, so it is unrealistic to expect security staff to check for the presence of these cameras in all their myriad forms, as this would likely incur a significant delay.

In this challenge, there is the requirement to develop a technical solution to rapidly disrupt or prevent recordings at pinch point entrances and exits of secure facilities. This must be done remotely (i.e., no physical access to the vehicle) while leaving no lasting impact that the dashcam recording has been interrupted, ensuring the owner has no adverse experiences from this effect.

Project scope

Working with the users in an agile approach, by the end of the project period there should be the aim to achieve at least a concept demonstrator achieving TRL 4 - technology basic validation in a laboratory environment. There is no prescribed route to achieve a concept demonstrator, approaches that could be considered are:

- Conduct a market trawl of prospective solutions that could either be used out of the box, or adapted to solve this challenge quickly and cost-effectively.
- Basic research to prove the principle in a lab environment that a dashcam can be safely interrupted, while minimising the intrusion on the owner.
- Using existing developments which can be pivoted to this use case to produce one or more demonstrable prototypes for prospective users to trial.

Proposals not within scope are those that require physical access to the inside of the vehicle, and solutions that have a lasting impact on the dashcam.

Dates

Competition opens	Monday 20 November 2023
Online briefing link	Wednesday 6 December 2023 at 10:00am
Clarifying questions published	Tuesday 19 December 2023
Competition closes	Thursday 11 January 2024 at 5:00pm

Applicant notified	Friday 26 January 2024
Pitch day in Milton Keynes	Thursday 1 February 2024
Target project kick-off	March/April 2024

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 OpTech Co-Creation challenges.

How we evaluate

All proposals, regardless of the application route, will be assessed by the OpTech 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 OpTech 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

OpTech 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.

Co-Creation Terms and conditions

Proposals must be compliant with the OpTech 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.

NSTIx OpTech Co-Creation Supporting information

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 About us - National Security Technology and Innovation Exchange - GOV.UK (www.gov.uk)).

FAQs

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

   As per the OpTech 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 OpTech 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 OpTech Co-Creation team as feasible, viable and desirable, then phase 2 funding will be made available.

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

Yes, in fact this is encouraged, and additional funding may be made available as per the outlined budget.

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

Yes, it will be made available to stream and view at your leisure after it has been broadcasted. This will be made available via the OpTech Co-Creation community collaborators.

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

There is no requirement for security clearances, our preference is work to be conducted at OFFICIAL.

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.

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

- Advice and guidance on how to keep your organisation secure online can also be found through the National Cyber Security Centre.
- Solution providers should also consider the protective security measures they have in place. Please ensure ways of working are in-line with Trusted Research (for academia) and Secure Innovation (for businesses) guidance.
- END.