HMGCC Co-Creation

Geolocation and detection of deepfakes from photos

Summary of the challenge

Tools to geolocate and detect deepfakes in photos are the focus of the latest HMGCC Co-Creation challenge now open for applications.

Organisations are being invited to apply for a 12-week challenge aimed at researching potential tools and their effectiveness.

Photo analysis is important to national security for example in a hostage situation, when images are scrutinised for clues to proof of life and location. Continuing developments in doctored photos and deepfakes have made this more challenging.

This project will be centred around two workstreams:

- 1: Test commercial photo geolocation tools, explaining how they work. The bulk of the work is expected in this workstream.
- 2: Conduct deepfake red/blue team testing.

Organisations are encouraged to collaborate and form consortia for these workstreams, particularly for red/blue team testing. Increased funding is available for these collaborations.

Technology themes

Artificial intelligence, app development, business intelligence, computer vision, data science and engineering, geospatial science and technology, machine learning, privacy enhancing technologies, software development.

Key information

Budget per single organisation, up to (ex VAT)	**£80,000**
Budget for consortium, up to (ex VAT)	**£120,000**
Project duration	**12 weeks**
Competition opens	**Monday 22 September 2025**
Competition closes	**Thursday 23 October 2025**

Context of the challenge

National security investigates images of concern, including those related to kidnappings, conflicts, suspected crimes, terrorist activity, and disinformation deepfakes. Photos are analysed to identify perpetrators and the location of the offence.

The gap

Although AI tools can help geolocate where a photo was taken using features within the image such as trees or vehicles, these black box style tools don't provide the reasoning of why a conclusion has been reached. Any checks are also being carried out against a backdrop of major advances in deepfake technology – making this work even more challenging.

Example use case for the intended tool

In an exercise examining images for 'proof of life' evidence in hostage scenarios, Jean is looking closely at photos of Claude. In a real situation, it would be her job to help gain information to aid his safe release.

In one photo Claude appears to be alone with a view of the road behind him as well as a wooded area and cloudy sky. There is no metadata or digital forensics information available to investigate. Jean uses a tool to analyse this image which suggests several locations with varying degrees of confidence suggested. The reason behind the conclusions from the tool are explained, giving a level of assurance. Jean looks to verify these locations with street view images.

In another image, the tool being used suspects the background image is not consistent with the road markings and the flora in view suggesting alternative locations. There is a flag from the tool that the image appears to have been altered or is entirely fake.

Using this tool, Jean can distinguish fake from real images, aiding in the successful re recover Claude from captivity.

Project scope

Applicants should aim to deliver a report of their research, and, if applicable, a developed geolocation deepfake detection image tool. The workstreams are:

- 1**:** Test commercial and in-development photo geolocation and deepfake detection tools, explaining how they work. The bulk of the work is expected in this workstream.
- 2**:** Conduct red/blue team testing of photo geolocation tools, using genuine and deepfake images to assess accuracy. It is encouraged that different organisations create photos and deepfakes (red team) and another detects (blue team). More funding is available for consortium submissions.

Tools being tested should range from mature technology readiness level (TRL) 9 to those in development, TRL 5. In addition, there is up to £10,000 of a further call-off budget towards purchasing of software licenses and tools.

Essential requirements

- Trial a minimum of four different geolocation and deepfake detection tools.
- Provide a final report on tools tested. Include detection methods analysed, indicators that are identified in images and how confidence/accuracy levels are determined.
- During red teaming, use deepfake generation that requires text or image input and not artistry techniques.
- Use geolocation tools that could operate without an internet connection.

Desirable requirements

- A geolocation tool which provides a confidence heatmap. For example, if a tree type suggests high confidence in pinpointing location but a road sign suggests low confidence.
- A geolocation tool with text-based input and interface.
- Details of the training data used by the geolocation tool.

Not required

- A tool that only scans metadata.

Dates

Competition opens	Monday 22 September 2025
Online briefing call	Tuesday 7 October 2025 at 10am

Online briefing link (Please note: Recording or use of AI notetakers is not permitted)	Teams Link
Clarifying questions deadline	Tuesday 7 October 2025 at 5pm
Clarifying questions published	Friday 10 October 2025
Competition closes	Thursday 23 October 2025
Applicant notified	Tuesday 4 November 2025
Pitch day in Milton Keynes	Tuesday 11 November 2025
Pitch Day outcome	Wednesday 12 November 2025
Commercial onboarding begins*	Friday 14 November 2025
Target project kick-off	Monday 1 December 2025

**Please note, the successful solution provider will be expected to have availability for a one hour onboarding call via MS Teams on the date 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.

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.

How to apply

Please submit your application on the HMGCC website. Any queries please email cocreation@hmgcc.gov.uk.

All information you provide to us as part of your proposal will be handled in confidence.

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

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.

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?**

   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, in fact this is encouraged, and additional funding may be made available. Please see the maximum budget of the individual challenge.

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

If a briefing event is held, any questions (and answers) will be captured and published after the event. The call itself is not recorded and use of AI notetakers is not permitted.

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.