HMGCC Co-Creation

Challenge: AI-enhanced x-ray imaging for bomb disposal

Summary of the challenge

Can you develop a machine learning-enabled solution that helps engineers identify, characterise, and understand electronic components using only x-ray images?

To safely disarm explosive devices, skilled operatives sometimes use x-ray images to identify the electronic trigger and disarm it. However, this is difficult with complicated circuits and when the images are not clear.

This is a 12-week funded challenge. Applicants must deliver a demonstrator at Technology Readiness Level (TRL) 5 within the project period.

HMGCC will provide funding for time and materials, overheads, and other indirect expenses for successful applicants.

Technology themes

Applied research, artificial intelligence, computer vision, data science and engineering, machine learning, non-destructive testing, software development.

Key information

Total budget (ex VAT), up to	£60,000
Project duration	12 weeks
Competition opens	Monday 28 September 2026
Competition closes	Thursday 12 November 2026

Context of the challenge

Bomb disposal is dangerous work undertaken by military and policing agencies among other government organisations. A key part of the process to safely disable a suspected explosive device while limiting physical contact, is using x-ray images to

OFFICIAL 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.

identify the electronic components that make up the switching mechanism designed to detonate a suspected explosive device.

This task can be further complicated by the presence of tripwires, anti-tamper mechanisms, and other countermeasures that may trigger the device if disturbed.

The gap

Analysing x-ray images of explosive devices is a highly specialised skill. Because specialists are not usually deployed in the field, operators on the ground must capture images and send them to remote experts for analysis and advice.

This process can be slowed down by poor-quality images taken under operational pressure, the need for additional imaging, and the time it takes to send large files over limited communications links.

Advances in artificial intelligence and machine learning, used to identify key electronic components in complicated circuits, could bring some of this analysis closer to the point of need. This could help operators identify and classify electronic components more quickly in the field, while ensuring human operators remain responsible for all operational decisions.

Example use case

Sergeant Heyland is a member of a specialised Explosive Ordnance Disposal (EOD) team deployed overseas.

While on patrol, he finds a suspected Improvised Explosive Device (IED). It looks complex, so the analysis is likely to be difficult. After securing the area, he takes x-ray images of the device from multiple angles to gather as much information as possible, then withdraws to a safe distance.

Using a newly deployed analysis tool, Sergeant Heyland processes the images himself, onsite. The software identifies and labels electronic components within the images, flags anything it is uncertain about and asks for further images to improve confidence in the assessment.

Once Sergeant Heyland provides these further images, the system identifies a range of electronic components and provides assesses their likely characteristics and functions and highlights any that may be critical to how the device works.

As this is safety-critical work, Sergeant Heyland still consults UK-based specialists. However, he can now send smaller, more focused information, so his questions are answered more quickly.

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.

This means Sergeant Heyland can complete his task more efficiently, while specialists continue to provide expert oversight.

Project scope

This challenge is about developing machine learning algorithms that can identify and label electronic components from x-ray images while assessing their likely function within a circuit.

Applicants should aim to deliver a demonstrator at a minimum of Technology Readiness Level (TRL) 5 (technology validated in a relevant environment) within the 12-week project period.

Essential Requirements

- Deliver a demonstration to the sponsors, along with the software, source code and a report detailing how it functions.
- Use machine learning techniques to identify and analyse electronic components
- Ensure the software can be used by trained operators who are not electronic component specialists
- Provide traceability and explainability for outputs.
- Show confidence scores for identified components and extracted information.
- Run on commercially available hardware.
- Support multiple data types, particularly TIFF and JPEG files
- Demonstrate identification and analysis of through-hole components, such as capacitors and resistors.

Desirable Requirements

- Support offline or disconnected operation.
- Support retraining or refinement using additional labelled data.
- Demonstrate identification and analysis of surface mount components, such as microcontrollers, capacitors and resistors.
- Generate structured reports suitable for technical assessment activities.

Constraints:

- Training data will be made available to the winning solution provider.
- Solutions should avoid reliance on proprietary datasets where possible.
- The solution must use x-ray images as its primary source of analysis.
- Solutions should provide evidence-backed outputs and clearly explain any uncertainty.

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.

Not required:

- A horizon scan.

Dates

Competition opens	Monday 28 September 2026
Clarifying questions deadline	Friday 16 October 2026
Clarifying questions published	Thursday 5 November 2026
Competition closes	Thursday 12 November 2026
Applicants notified	Tuesday 24 November 2026
Pitch Day	Wednesday 2 December 2026
Pitch Day outcome	Monday 7 December 2026
Commercial onboarding begins*	Friday 11 December 2026
Target project kick-off	January 2027

*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:

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.

Feasibility	• What is the technical credibility of the minimum viable product proposed?
	  ○ Is it technically possible?
	  ○ Are there key technical risks overlooked?
	• Likelihood of the minimum viable product reaching or exceeding the minimum required Technology Readiness Level (TRL)?
	  ○ Does the proposal aim to reach the minimum TRL?
	  ○ Assessors' confidence in the proposal from technical perspective?
	  ○ Will the proposal exceed the minimum TRL?
	• Credibility of the team regarding technical and project management skills?
	  ○ Does the team have all the relevant expertise?
	  ○ How experienced are they?
	  ○ Have they delivered something similar before?

Desirability	• How closely does the proposal directly address the challenge?
	  ○ Does the proposal achieve all essential requirements?
	  ○ How many desirable requirements are achieved?
	  ○ Is this something the user's want?
	• How well is the benefit for government and dual-use described?
	  ○ Is the benefit to the user's well described?
	  ○ Have the applicants identified dual-use markets?
	• Ambition of the proposed solution?
	  ○ Does the solution provide an incremental step in capability or significant leap?
	  ○ Is the proposed solution unique to the applicants?

Viability	• How well is the exploitation route described?
	  ○ Is the proposal just aiming to deliver the minimum for the project? Or have they got a project plan post phase 1?
	  ○ Are they thinking about commercial exploitation routes?
	  ○ Are there rough costings for future work?
	• How well does the proposal demonstrate value for money and are the costs broken down and justified?
	  ○ How much time and resource is spent on a project for the cost?
	  ○ Is there a perceived high ambition for the cost?
	  ○ Is there a robust costing plan?

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.

	• How well is the project delivery described leading to the minimum viable product?
	  ○ Is there a Gantt chart or similar?
	  ○ Are there proposed outcomes after each sprint?
	  ○ Are the applicants experienced in Agile methodology?

Budget	• Are the project finances within the competition scope?

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 before the deadline with the challenge title as the subject. 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 Co-Creation website. Any queries please email Co-Creation@dstl.gov.uk and cocreation@hmgcc.gov.uk.

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

Applications **must** be no more than six pages or six slides in length. HMGCC Co-Creation reserves the right to stop reading after six 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:

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.

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

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.

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. **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.

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.

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. **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.

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.