HMGCC Co-Creation

Smart personal assistant for security researchers

Summary of the challenge

Can you help us unlock faster, smarter vulnerability insights?

When machinery is procured to support national security and defence it has to be thoroughly checked for security vulnerabilities — and those vulnerabilities need to be understood and addressed. The work depends on highly skilled security researchers who assess vulnerabilities and advise on mitigations. But before the expert analysis can begin, there's a significant bottleneck: finding, indexing and understanding the vast amount of open-source technical information that exists about complex industrial machinery.

HMGCC Co-Creation are launching this challenge to develop a software tool to Technology Readiness Level 6, that works without an internet connection and can assist a security researcher to index, search and understand vast quantities of data faster, enabling faster decision making.

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

Technology themes

Artificial intelligence, app development, cybersecurity, data science and engineering, information technology, machine learning, software development, threat modelling, vulnerability research.

Key information

Total budget (ex VAT), up to	£60,000
Project duration	12 weeks
Competition opens	Monday 16 March 2026
Competition closes	Thursday 7 May 2026

Context of the challenge

National security organisations undertake sensitive activities but also depend on complex supply chains to acquire and maintain the technology they need to operate. As part of that, security researchers carry out detailed tear-downs examining software, hardware and data components to identify possible vulnerabilities.

The first stage of this process is research. When a security researcher is tasked to examine a new product, particularly in the context of industrial control systems, they need to draw on open-source information at a micro-component level, such as technical specifications, datasheets, schematics and technical forum discussions. It is laborious and takes time that could be better spent on the analysis itself.

This challenge is about changing that. We believe that human-machine teaming offers a real opportunity to reduce the research burden. Specifically, we are looking for a system that can do three things:

- Index both structured and unstructured technical information about a product and its components.
- Generate a clear technical summary of the product and its individual components.
- Allow the researcher to ask natural-language questions about the product and explore the information interactively, adapting their line of investigation as new information emerges.

The gap

Industrial control systems can be highly complex and thus time consuming to index and query related information. Complexities can arise from the following:

- Products vary significantly, meaning there is no one size fits all.
- There can be multiple product versions with varied components and software updates.
- Security researchers rely on their experience, processes and trusted sources, such as information directly from the vendor and trusted online forums.
- A chain of trust is formed from:
    - Physical components such as filters, fuses, processors and memory sensors.
    - Software across a range of forms including source code or binary for multiple different processors and operating systems in the same product.

Example use case

Alicia is an experienced security researcher with a focus on industrial control systems. She has been tasked to assess an industrial additive manufacturing machine. The machine will be used in a manufacturing facility without an internet connection, to build critical, classified, components for national security and defence operations. Any vulnerabilities must be understood and mitigated.

She begins with the vendor manual, supplied in paper copy and PDF.

Using the wiring diagram and schematic she starts to investigate the hardware architecture, including interfaces and components and microprocessors. She sources datasheets online for each component and also finds photos of various tear-downs.

She starts to pull-out all the available code supplied by the vendor.

She consults online forums, some trusted and some are new to her.

Alicia starts to build up a large library of information on the product and its components. She drags and drops each bit of information into her ‘tear down assistant’ tool.

As she builds this library of information, she naturally starts to learn about how the machine works, but she also needs to be able to call back on this vast amount of information efficiently. An intelligent, easy to use search and summary capability is essential.

When she wants to explore the machine's interfaces, she types a query into the tool and receives a conversational response, backed by a reliable source. She builds on this with follow-up questions, each time receiving a well-grounded answer, citing sources. Where answers are not clear, this is highlighted with alternative theories. As the assistant starts to learn Alicia’s behaviour, it adapts to her needs.

This operates more than just a search tool but is more like a personal assistant who really understands the subject matter, and Alicia.

Project scope

This challenge focuses on building a standalone software tool that can ingest relevant open-source information, compile it into a searchable library, support natural language queries across multi-modal formats and provide conversational intelligent and well-informed answers. We would like to see proposals which don’t just focus on off the shelf Retrieval-Augmented Generation systems.

After the 12-week project, the final deliverable should be a software tool meeting the stated requirements for testing in-house at HMGCC.

Essential requirements:

- The tool must have the ability to understand system architecture of a selected machine. A non-exhaustive list of components to understand are the physical interface interactions, data interfaces and protocols.
- Have an ability to check and validate responses before publishing, to prevent erroneous information and hallucinations.
- Characterise from multimedia inputs, such as including manuals, schematics, datasheets, corporate databases, images, code, handwritten annotations.
- Verify information by listing sources and cross checking against high confidence data such as industry publications, academic research and manufacturer documentation.
- Flag a confidence score and if more source data is required.
- The solution should be capable of operating on a laptop without an internet connection, allowing users to characterise complex systems and identify vulnerabilities in environments with limited or no connectivity.
- Provide an easy to search and intelligent function to query the dataset in a chat-like manner.
- Keep a memory of queries so conversations can be continued over several weeks without repetition of prompts.

Desirable requirements:

- Build a profile of the user and adapt to their needs, for example to present information in preferred formats and even proactively provide information that is frequently requested.
- Ability to translate and index non-English data sources (e.g. datasheets and forum posts).
- Recognise and mitigate cultural biases to ensure a nuanced understanding.
- Ensure the software tool remains up-to-date when offline. Consider in a future iteration how the solution may incorporate a mechanism for periodic updates of the core tool and its indexing/search algorithms.

Constraints:

- The tool must work without an internet connection.

Not required:

- For this challenge, the system does not need to autonomously identify or search for source data (e.g. datasheets, schematics and forum posts). Test data will be provided.

Dates

Competition opens	Monday 16 March 2026
Briefing Call [MS Teams link here]	Friday 17 April 2026
Clarifying questions deadline	Friday 17 April 2026
Clarifying questions published	Tuesday 28 April 2026
Competition closes	Thursday 7 May 2026
Applicants notified	Friday 22 May 2026
Pitch Day	Tuesday 2 June 2026
Pitch Day outcome	Monday 8 June 2026
Commercial onboarding begins*	Friday 12 June 2026
Target project kick-off	July 2026

*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:

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? • 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.

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.

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?**

   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.

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.