HMGCC Co-Creation

Challenge: Mobile mimicry using AI

Summary of the challenge

Can you build an AI agent that behaves like a normal phone user to make testing easier and faster? We want to be able to automate the process of testing modified software on large numbers of mobile phones at once. The testing must be thorough, covering all possible situations and use cases.
We are seeking Technology Readiness Level 5 demonstrator within 12 weeks.

HMGCC Co-Creation will provide funding for time, materials, overheads and other indirect expenses for applicants successful in phase 2 of the competition.

Technology themes

App development, business intelligence, communication systems, cybersecurity data science and engineering, digital services, information technology, software development.

Key information

HMGCC Co-Creation will be hosting a two-stage competition process.

Phase 1. The objective is to rapidly assess one-page proposals, no feedback will be given at this stage. Successful applicants will be invited to phase 2. For further information please see **How to apply – phase 1.**
Phase 2. Successful phase 1 applicants will be requested to submit a proposal directly to cocreation@hmgcc.gov.uk. For further information please see **How to apply – phase 2.**

Total budget (excluding VAT)	£60,000
Project duration	12 weeks
Phase 1 Competition opens	Monday 21 September 2026
Phase 1 competition closes	Thursday 8 October 2026
Applicants notified	Monday 19 October 2026
Phase 2 competition opens	Monday 19 October 2026

Phase 2 competition closes	Thursday 29 October 2026

Context of the challenge

National security engineering organisations regularly produce bespoke software for specialised deployments. This includes deploying software onto modified hardware, including mobile phones.

These devices are often used in critical missions, where failure is not an option. Testing on deployed devices must be thorough and robust. Industry will often do this using phone testing farms. We know employing AI agents could make this task easier.

This challenge is focussed on deploying AI agents onto mobile phones to replicate normal phone usage at scale.

The gap

Agent AI can already imitate human behaviour in many domains and work with a degree of autonomy for some tasks. Many sectors are looking to integrate these systems into workflows.

But few have been deployed on mobile devices. We need an AI agent that can mimic human behaviour patterns. It must be able to:

- Connect to a network
- Have some pre-trained personas to mimic a variety of different natural behaviours, including accessing web pages and sending messages.
- Replicate those habits at human-like speed, not machine-speed.

Example use case

Alayna is a team leader in a software development team creating bespoke software for mobile phones.

As part of testing and verification, she needs to build confidence that a phone still operates without bugs in a variety of different operating conditions, for example with varying user experiences and environmental conditions.

She uses a test environment in which different conditions can be simulated including GNSS positioning, network and WIFI access points, and environmental conditions such as temperature.

She also needs multiple phones to be used in different ways to simulate different use cases. Previously, this may have been done by test engineers virtually controlling

these phones with pre-defined use cases – but what about when large numbers of phones have to be tested at once?

Instead, Alayna installs MIMIC (Mobile Intelligence Managing Individual Conduct) – an AI agent on each phone. Different personas can be selected which simulate real-world use cases. Each phone is used exactly as it would be by a person, from accessing website, using map services, to sending messages. With MIMIC installed, realistic phone usage is replicated at a speed never achieved before.

Project scope

Develop an AI Agent tool that can operate autonomously on a mobile device (or virtual surrogate) to mimic a person.

The outcome should be a demonstrator after this 12-week project, to a minimum Technology Readiness Level (TRL) 5 – technology basic validation in a relevant environment. The software should be demonstrated to the sponsor with a detailed report.

Essential requirements:

- The AI Agent should be demonstrated operating in an emulated environment.
- Must provide source code and a detailed technical report.
- Installation and operation must require no technical expertise.
- The agent runs unsupervised in training; a human can intervene during operational use.
- The project must demonstrate appropriate guardrails, including explainability of AI agent autonomy and robustness of cybersecurity.
- Must be able to send SMS, use messaging apps and place voice calls.
- Solution must make it possible for variety of personas to be selected.
- Able to route traffic through configurable VPN exit nodes.

Desirable requirements:

- Run on a physical mobile phone (not just an emulation).
- Target the smallest, most powerful efficient model available.

Constraints:

- Testing will take place in an on-premises environment.
- No training data will be provided.

Not required:

- Natural language phone conversations.
- Horizon scanning.
- Low TRL research

Dates

Phase 1 competition opens	Monday 21 September 2026
Clarifying questions deadline	Monday 28 September 2026
Clarifying questions published	Monday 5 October 2026
Phase 1 competition closes	Thursday 8 October 2026
Applicants notified	Monday 19 October 2026
Phase 2 competition opens	Monday 19 October 2026
Phase 2 competition closes	Thursday 29 October 2026
Applicant notified	Tuesday 10 November 2026
Pitch day in Milton Keynes	Thursday 19 November 2026
Commercial onboarding begins*	Friday 27 November 2026
Target project kick-off	December 2026/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 to apply – phase 1

Please submit your application on the HMGCC Co-Creation website. Any queries please email 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 one page or one slide in length. HMGCC Co-Creation reserves the right to stop reading if this limit is breached. The page/slide limit excludes title pages, references, personnel CVs and organisational profiles.

Phase 1 applications will be assessed using the following scoring criteria:

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 users want?
	• How well is the benefit for government and dual-use described?
	  ○ Is the benefit to the users 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?
	  ○ Does the solution introduce a new idea?

Following assessments, the successful applicants will be invited to submit a more in-depth proposal in phase 2.

How to apply - phase 2

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.

Phase 2 applications will be assessed using the following scoring 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?

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.

	○ 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 users want? • How well is the benefit for government and dual-use described? ○ Is the benefit to the users 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 are 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 phase 2 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.

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.

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.

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.