HMGCC Co-Creation

Challenge: NCA seeks emulated phone technology to help combat crime

Summary of the challenge

Emulated phone technology is being sought by the National Crime Agency (NCA) to support its work using multiple aliases to communicate with numerous people nationally and internationally.

In its latest challenge, HMGCC Co-Creation wants to hear from organisations which have an emulated phone solution to potentially help the NCA in its future work.

The solutions being put forward by organisations applying for this challenge should already be at mid to high Technical Readiness Level (TRL).

Organisations are being asked to apply if, over a 12-week period, they can develop and demonstrate a piece of technology to meet this challenge. HMGCC Co-Creation will provide funding for time, materials, overheads, and other indirect expenses.

Key information

Budget up to	**£60,000**
Project duration	**12 weeks**
Competition opens	**Thursday 10 October 2024**
Competition closes	**Thursday 7 November 2024 at 17:00hrs**

Context of the challenge

This HMGCC Co-Creation challenge, launched on behalf of the NCA, is looking for an emulated phone solution.

The NCA's mission is to protect the public from serious and organised crime. It operates across the UK and around the world. This requires NCA officers to be able to communicate securely, effectively and dynamically with officers and a range of partners 24/7, 365 days a year. Communications include voice, text, video and picture messaging.

Officers may use multiple aliases and several physical mobile phones to interact with numerous people, protecting their identity and the identity of those with whom they

communicate. The NCA wants to reduce the use of physical handsets, in favour of simplifying operations by using a single approved device. The single device should be able to host a series of emulations that can be spun-up and decommissioned rapidly. Due to the sensitivity of some operations, there must be minimal risk of emulation being linked, and any risks should be identified and clearly articulated for the risk owner.

The gap

When applying for this challenge, please consider the following questions and how a solution relates to them:

- Could an officer use your solution to run multiple different aliases, with minimal contagion risk?
- Can the solution be used within a secure government facility where mobile phones may be prohibited?
- What are the running costs and maintenance overheads?
- Does this simplify the users' experience compared to using multiple non-traceable phones?
- Would its use look normal for a plain-clothed officer, for example during transit through an airport?
- Is there a risk of exposing identities within the phonebook?

Example use case

Leo is an operational officer deployed overseas to investigate serious and organised criminals targeting UK victims.

Leo carries with him multiple non-traceable UK issued phones so he can communicate with different suspected criminals as well as law enforcement colleagues, using distinct and separate aliases.

Leo travels successfully through the airport but is aware that carrying multiple phones may look suspicious. Whilst abroad, Leo is on call 24/7 and has the overhead cost of maintaining each phone, as well as the responsibility of ensuring he is using the right phone to contact the right person, using the correct alias. The whole process needs to be streamlined, less subject to risk and benefit from cost savings by reducing the number of phones for each operation.

Leo gives his requirements to Jenny, a technical solutions architect. Jenny identifies a work issued device as a solution which can message physical phones owned by suspected criminals or law enforcement colleagues with minimal risk of digital contagion across each interaction. This would allow Leo to use multiple aliases with

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

reduced maintenance cost and less potential for error. Jenny's solution is agile and repeatable and can direct calls to officers 24/7, so Leo can use the same device.

Project scope

Applications should already have partially developed emulation capability. The output of the 12-week project should be a demonstration of running mainstream apps through emulation, achieving at least TRL5.

Applicants should consider the below list of requirements for consideration in the final solution:

Constraints:

- Current focus on Android software only
- Must be able to use mainstream and bespoke apps
- Persistent account and data within apps
- Solutions must consider encryption

Desirable features:

- Use of the cloud
- Visual and audio input can be fed into the device
- Could consider using Mobile Virtual Number Operator (MVNO)
- Agility of alias generation so they can be commissioned and decommissioned rapidly
- Keystrokes and interaction may be used for evidential purposes in the future
- Alias generation must exhibit a realistic pattern of life, geolocation, SIM card properties etc.

Stretch targets:

- Alert system for the user to check messages on the emulator

Solutions should not include the following:

- Remote control or the need to purchase multiple mobile phones
- Horizon scanning

Dates

Competition opens	Thursday 10 October 2024
Deadline for questions	Tuesday 22 October 2024

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

Clarifying questions published	Tuesday 29 October 2024
Competition closes	Thursday 7 November 2024 at 17:00hrs
Applicant notified	Monday 18 November 2024
Pitch day	Tuesday 26 November 2024
Target project kick-off	Monday 6 January 2025

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?

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

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 publication 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

HMGCC 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.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

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.

HMGCC 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 HMGCC 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 is part of the NSTIx Co-Creation network, which enables the UK government national security community to collaborate on science, technology and innovation activities and to deliver these in partnership with a more diverse set of contributors for greater shared impact and pace.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

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?**

   For this challenge, one solution provider will be funded, based on 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?**

   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, multi-disciplinary consortiums are encouraged. But please note there are budget restrictions outlined in key information, depending on the challenge there are sometimes higher budgets made available for consortiums.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.

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.

Disclaimer: This information may be exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK legislation. Refer disclosure to the originating department.