HMGCC Co-Creation

Challenge: eSIM reader for officer safety

Summary of the challenge

Single organisations can apply for up to £60,000 of funding, for an agile 12-week project to show the feasibility of gathering an IMSI identifier from an electronic SIM card (eSIM) for the purposes of national security officer safety. This is 100% funded by HMGCC Co-Creation for time and materials. There is potential for multiple projects to be funded.

Key information

Budget per single organisation, up to	**£60,000**
Budget per consortium, up to	**£120,000**
Project duration	**12 weeks**
Competition opens	**Monday 4 December 2023**
Competition closes	**Thursday 1 February 2024 at 5:00pm**

Context of the challenge

National security has a requirement to read IMSI numbers from mobile phones and other small electronic devices that members of staff use, ensuring we have duty of care. Existing techniques include removing the physical SIM card from the device and placing it into a reader that interrogates the card and displays its IMSI number.

The gap

There is a rapidly increasing prevalence among mobile phone manufacturers to move away from using removable SIM cards in favour of embedded or integrated SIMS (eSIM). The iPhone 14 sold in the US, for example, no longer has a physical SIM card holder, but uses an eSIM instead. It's anticipated that many other manufacturers will also transition from physical SIM cards to eSIMs in the near future. Commercial software solutions are able to read eSIMs but they also collect collateral data, such as contact lists and SMS messages in addition to IMSI numbers, which is unacceptable for this scenario as it contravenes data handling regulations. There is therefore, no currently no acceptable means to read and record IMSI numbers from the emerging generation of eSIM enabled mobile phones and devices

Example use case

Jennifer, who is a Government employee is about to be deployed overseas to a friendly country. She could be there for months or years. Prior to travelling overseas, she has a long checklist to complete so she is well prepared. One of these is to provide her mobile phone IMSI number to the security officer, Robert, who will record this in corporate records.

When Jennifer is deployed, in case of emergency, her IMSI may be used to track her last known locations by providing the IMSI to local telecoms providers that the Government has good and well-established relationships with.

Robert and Jennifer discuss using Apps to find her phone, which are readily available, but there is little assurance with what is done with this data. Jennifer hands her phone over to Robert, but she has a modern phone with a non-removable eSIM. Robert hasn't got the equipment to read the IMSI as he's used to popping out a removable SIM card and placing in a SIM reader. He needs a secure and non-intrusive solution to easily and privately read the eSIM IMSI.

Scope

Below is a list of desirable functions:

1. The solution(s) must be able to read and display IMSI numbers from a wide range of unlocked mobile phones that utilise eSIMs.
2. Where more than one eSIM is active within a given mobile device, the solution(s) must be capable of reading and displaying the IMSI number for each SIM.
3. The solutions(s) should read and display the IMSI number of the phone of interest, only, and no other data from this phone nor any data, at all, from other phones, nearby.
4. The solution(s) must not pose a risk of damaging or corrupting the device being read or its associated eSIM.
5. The solution(s) should be intuitive to use, such that non-technical people can read and record IMSI numbers, effectively, with little or no training.
6. It is also desirable, for the solution(s) to read and display IMSI numbers from conventional SIM cards and satphone equivalents in addition to those from eSIMs

We are interested in developing innovative technology to approximately TRL 5 or 6, that can take an IMSI reading from an eSIM device (device agnostic) without taking collateral information. We are not prescriptive on the format of the concept demonstrator. But it must comply with data protection and GDPR, data aggregation must be considered and handled securely.

We are not interested in horizon scanning, technology mapping or low TRL developments.

Dates

Competition opens	Monday 4 December 2023
Online briefing link	Tuesday 9 January 2024 at 10:00am
Clarifying questions published	Monday 22 January 2024
Competition closes	Thursday 1 February 2024 at 5:00pm
Applicant notified	Friday 16 February 2024
Pitch day in Milton Keynes	Thursday 22 February 2024
Target project kick-off	March 2024

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.

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.
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 work 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 aim 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. This is a wide range of different UK government departments which will vary 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, 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 will 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 as per the outlined budget.

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

Yes, it will be made available to stream and view at your leisure after it has been broadcasted. This will be made available via the HMGCC Co-Creation community collaborators.

9. **Do we need security clearances to work with HMGCC Co-Creation?**

There is no requirement for security clearances, our preference is work to be conducted at OFFICIAL.

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.

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

- Advice and guidance on how to keep your organisation secure online can also be found through the National Cyber Security Centre.

- Solution providers should also consider the protective security measures they have in place. Please ensure ways of working are in-line with Trusted Research (for academia) and Secure Innovation (for businesses) guidance.

- END.