HMGCC Co-Creation

Challenge: Managing cyber-security risk through network monitoring

Summary of the challenge

Cybersecurity is key as adversaries continue to exploit public and private sector networks. Network monitors and penetration testing are one layer in this defence.

HMGCC Co-Creation is launching a 12-week challenge to find organisations able to develop a small, low-power, low-cost network monitor to improve observability and allow network packet modification for penetration testing.

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

Technology themes

Business intelligence, cloud computing, cybersecurity, data analytics, electronic engineering, information technology, software development, systems engineering, telecoms.

Key information

Budget per single organisation, up to (ex VAT)	**£60,000**
Project duration	**12 weeks**
Competition opens	**Monday 20 October 2025**
Competition closes	**Thursday 20 November 2025**

Context of the challenge

All organisations are aware of cybersecurity risks, with several recent high-profile cases. There are numerous online guidance and resource documents to help organisations protect themselves, notably published by the National Cyber Security Centre.

To protect the UK government against potential risks and new attacks, greater visibility and network testing are required. To enable this, the use of low size and cost network monitors is being explored. These would enable advanced penetration testing capabilities to be used against networks including packet manipulation as well as increasing network visibility.

The gap

There are some existing tools that can directly monitor network traffic, but these are typically targeted towards large operators and are scaled for much higher network volumes than is needed for this use case, resulting in higher price tags. There is a requirement to develop a low size, weight and power variant, which can operate within small data centres. It should also be low-cost to encourage wider adoption.

The critical technical requirement is a network pass-through (optical or copper) that allows the network to be unaffected by the network monitor, even if the network monitor were to fail in operation.

Example use case

To guard against potential hacking attempts, a security operations centre is working with a team to monitor network traffic to and from a government estate. As part of increased security, they also plan to carry out regular penetration tests on the network, to ensure it is protected.

Kay's team is trialling a new network monitor to observe traffic at source. If successful, Kay will roll this out to other sites. Even though this is a test, it would cause serious impact if the network monitor disrupted internet connection.

Part of Kay's team are specialist network engineers to ensure correct installation. They are working late at night to minimise disruption. The installation area is cramped for space, can get quite hot, but at least does have easy access to AC mains.

Once installed successfully the data link is passed to the security operations centre.

Kay's team also has the option to inject modified packets to simulate malicious traffic. This penetration test is caught by the firewall, confirming a successful outcome for the security operations centre.

At some point during operation, the network monitor fails. It is later discovered that there was a minor manufacturing defect that only caused an issue after some time. However, this proved a successful trial as, during failure mode, the fail-safe pathway allowed data to bypass the network monitor without incident.

Project scope

Applicants should aim to deliver a demonstrator and report in this 12-week project. This is open to Technology Readiness Levels (TRL) from 5 – 9. It is recommended that proposals label both the existing TRL and the TRL expected by the end of the 12 weeks. Critical, essential and desirable requirements are listed, along with constraints and what is not required.

Critical requirement:

- Must incorporate an optical or copper pass-through, so if the device fails it does not affect normal network traffic.

Essential requirements:

- Deliver a physical demonstrator at the end of the project, for further testing by the sponsors.
- Operating temperature range of -10C to +60C.
- Low size, weight and power (SWaP) must be considered, and if not achievable in the 12-week project a roadmap must be presented to achieve this in the future.
    - Ideal size is less than 1 litre.
    - Ideal power is less than 45W, from mains AC.
- Processor must be capable of bi-directional 10Gb bandwidth.
- Copper network input or fibre network input
- Multi-mode and single mode network.

Desirable requirements:

- Ideal Ingress Protection rating is IP66.
- Consider relatively low cost for final unit price, a price over £5,000 may be prohibitive.
- Consider the mechanism to program a unit. The sponsors of this challenge will work with the solution provider on preferences and software package trade-offs.
- Copper network input and fibre network input in the same unit.
- Consider robust and rugged used units, however this is largely out of scope for this phase of the project.

Constraints:

- Operation within a small data centre.

Not required:

- Horizon scanning only.
- Large bulky and high-cost units.
- Not just a passive tap or span.

Dates

Competition opens	Monday 20 October 2025
Clarifying questions deadline	Tuesday 4 November 2025
Briefing Call - **Registration Link** (Please note: Recording or use of AI notetakers is not permitted)	Tuesday 4 November 2025 at 10am
Clarifying questions published	Tuesday 11 November 2025
Competition closes	Thursday 20 November 2025
Applicant notified	Wednesday 3 December 2025
Pitch Day in Milton Keynes	Thursday 11 December 2025
Pitch Day outcome	Monday 15 December 2025
Commercial onboarding begins*	Tuesday 6 January 2026

Target project kick-off	Mid to late January 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:

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 co-creation@dstl.gov.uk and 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 proposal, whether submitted directly or via a collaborator platform, will be handled in confidence.

Applications **must** be no more than six pages or six slides in length. HMGCC Co-Creation reserve 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:

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 fund 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 two 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 one - 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.