HMGCC Co-Creation

Challenge: Security watermarks for physical documents

Summary of the challenge

A 12-week challenge has been launched by HMGCC Co-Creation, looking for ways to add bespoke watermarks to physical documents.

The ability to do this without needing large-scale manufacturing runs could prove an important tool in national security, to combat forgery.

Organisations are being invited to apply for this funded challenge to develop new processes and manufacturing concepts, enabling small-scale, agile production runs of security watermarked documents. The goal is to create a flexible and responsive system that can quickly adapt to new security requirements.

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

Technology themes

Engineering design consultancy, facilities, manufacturing, materials science and engineering, model prototyping, systems engineering.

Key information

Budget per single organisation, up to	**Up to £60,000 (ex VAT)**
Project duration	**12 weeks**
Competition opens	**Monday 6 October 2025**
Competition closes	**Thursday 6 November 2025 at 5pm**

Context of the challenge

Watermarks in physical paper documents have been an important security feature for centuries to signify authenticity and discourage counterfeiting. Watermarked

documents are ubiquitous, appearing in banknotes, passports, driving licences, certificates, and other official documents handled daily by the public.

However, there are special cases where official paper documents are issued and an agile capability to produce watermarks is essential.

Applicants are also encouraged to identify commercial exploitation opportunities.

The gap

Creation of watermarks involve two primary processes:

- **Watermarking during paper manufacturing**: Techniques like cylinder mould watermarking, UV-activated threads, and planchettes can be employed. While these methods offer enhanced security, they are complex and require large-scale manufacturing processes.
- **Post-processing of prepared paper**: A dandy or impression roll is used to emboss a 2D pattern. Although this method is simpler and more common, it is also more vulnerable to replication by counterfeiters.

HMGCC Co-Creation is launching this challenge to gain the best of both processes. By leveraging advanced manufacturing and using innovative methods for producing paper watermarks, it is believed that high precision, consistent and robust security features could be achieved, but in small production runs that are agile so easily changeable.

Example use case

In the event of a disinformation campaign launched by an adversarial group against the UK, the public's ability to distinguish between genuine and fake information may become compromised. While digital watermarking exists for digital media, physical document watermarking is required to become more agile for this threat.

Production engineer Gwen is tasked with increasing the number of watermarked documents, focusing on smaller production runs of government documents, from low-level public-issued leaflets to official paper documents shared within government. Mass produced documents such as passports, will not be affected by this change.

Gwen needs to cater to diverse customers with varying and bespoke requirements. She needs machinery that can automate the watermarking process, ensuring high precision and repeatability, while also handling diverse document types and quantities.

Project scope

Applicants should aim to deliver a process or manufacturing concept demonstrated in a relevant environment (Technology Readiness Level 5) within this 12-week project. Essential and desirable requirements are listed, along with constraints.

Essential requirements:

- Ability to apply complex watermarks into prepared ‘UV dead’ paper.
- Ability to process batch runs of up to 5,000 sheets of paper.
- A high precision, repeatable process is needed, not requiring artisan skills.
- Ability to easily change for the production of new watermarks at short notice.

Desirable requirements:

- Work on a number of different techniques, de-risk and recommend the most viable process.
- Consider techniques such as embossing, laser ablation, chemical etching, UV fibres, mylar threads, and others.

Constraints:

- It is unlikely that in the short term the sponsors could house new, large and expensive equipment, so low size, weight and power (SWaP) is important.

Dates

Competition opens	Monday 6 October 2025
Clarifying questions deadline	Tuesday 21 October 2025
Clarifying questions published	Tuesday 28 October 2025
Competition closes	Thursday 6 November 2025 at 5pm
Applicant notified	Friday 14 November 2025
Pitch day in Milton Keynes	Thursday 20 November 2025
Pitch Day outcome	Monday 24 November 2025

Commercial onboarding begins*	Thursday 27 November 2025
Target project kick-off	Monday 5 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 cocreation@hmgcc.gov.uk and Co-Creation@dstl.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 website. Any queries please email cocreation@hmgcc.gov.uk and Co-Creation@dstl.gov.uk.

All information you provide to us as part of your proposal 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.

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.

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. **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.

8. **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.

9. **Can you explain the Technology Readiness Level (TRL)?**

   Please see the UKRI definition for further detail.

10. **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.