



Challenge: Hidden stab vests for women

Summary of the challenge

Can you develop discreet, wearable stab-resistant body armour specifically designed for women?

Officers working in close protection units need to stay unseen and blend into the crowd, but they also need to protect themselves against possible attack. In this challenge we are focusing on finding the best hidden stab vests for women working in these jobs.

We are interested in technologies, materials and garment designs that could provide effective protection against sharp bladed weapons, developed to a minimum technology readiness level 5 and designed for women from the outset.

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

Technology themes

Applied research, healthcare, manufacturing, materials science and engineering, mechanical engineering, physical security, wearable technologies.

Key information

Total budget (ex VAT), up to	£60,000
Project duration	12 weeks
Competition opens	Monday 5 October 2026
Competition closes	Thursday 5 November 2026

Context of the challenge

Close protection officers who are charged with protecting VIPs from potential threats need to keep a low profile. Personal protection equipment, specifically stab and

slash proof body armour is a necessity. It must not draw attention, restrict movement or interfere with the officer's ability to blend into professional and social settings.

The commercial market has many protective garments available for men, designed around male body shapes but, whilst some options exist for women, female officers are still reporting compromises in comfort, fit, concealability and wearability.

The gap

Current protective garments are often made of plated material or woven aramid fibres. Although more body armour for women has appeared on the market in recent years, further solutions are still needed in the area of ultra low-profile and discreet stab vests to wear under clothing. Challenges faced include excessive bulk beneath lightweight clothing, reduced comfort during extended wear, restricted mobility and compromised fit for female users.

There is a need for innovative protective solutions that balance discreet appearance, user comfort and protection against edged weapon threats, while meeting the Home Office Body Armour standard 2017 or equivalent.

Example use case

Amelia and Frank are close protection officers supporting a VIP during a multi-day overseas visit.

Their role requires them to remain close to the principal, ensuring their safety. During this visit Amelia and Frank are wearing professional attire. Part of the job is to blend into a range of environments including meetings, receptions and public engagements.

They don't want to draw any attention to themselves or to frighten nearby public into thinking there could be danger, so they stay low profile. They may spend long periods standing, walking, driving and moving through crowded locations.

Amelia and Frank actually wear very similar protective equipment, concealed beneath lightweight business attire. Frank finds his movement largely unrestricted and remains comfortable throughout the working day, whereas the protective equipment for Amelia causes discomfort over time.

There needs to be a better solution so that Amelia remains protected against edged weapon threats, but her long term comfort needs are also met.

Project scope

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.

This challenge seeks prototypes of discreet stab resistant protection for female users.

The outcome should be to a minimum of Technology Readiness Level (TRL) 5 – technology basic validation in a relevant environment.

Essential requirements:

- A minimum deliverable of a swatch of the proposed protective material.
- A delivered final report, detailing performance, limitations and future development opportunities.
- Must be designed specially around female users.
- Must be designed for comfort and concealability under clothing.
- Must be stab and slash proof.
- Must provide a demonstration of effectiveness against bladed weapons
- Must provide at least a roadmap to achieve Home Office Body Armour standard 2017.
- Must use the guide – BSI 30417 Provision of inclusive personal protective equipment.

Desirable requirements:

- Demonstrate multiple protective equipment options to users for down-selection.
- Deliverable should include a wearable demonstrator.
- Consider trade-off of armour plates and fibres against performance, concealability and comfort for female users.
- The weight of protective equipment should be below existing commercially available protective solutions.
- The protective equipment should have enhanced breathability and thermal comfort.
- The protective equipment should be compatible with a range of body shapes and sizes.
- A stretch goal is to provide ballistic protection against handgun calibre projectiles.

Constraints:

- User comfort should be considered a primary design driver alongside protection
- Designs should consider practicality, maintenance and scalability

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.

- For continued work, the eventual product must be compatible with the Home Office Body Armour standard 2017 or equivalent

Not required:

- Overt, military style tactical body armour
- Concept studies without a demonstrator

Dates

Competition opens	Monday 5 October 2026
Clarifying questions deadline	Thursday 22 October 2026
Clarifying questions published	Thursday 29 October 2026
Competition closes	Thursday 5 November 2026
Applicants notified	Monday 16 November 2026
Pitch Day	Thursday 26 November 2026
Pitch Day outcome	Monday 30 November 2026
Commercial onboarding begins*	Friday 4 December 2026
Target project kick-off	December 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

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.

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:

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? ○ 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 user's want? • How well is the benefit for government and dual-use described? ○ Is the benefit to 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 is spent on a project for the cost?

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.

	○ 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 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 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 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 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.

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.

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.

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.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by using 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. 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?

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.

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.

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.