Helping the military shrink its cyber attack surface

The defence sector is diverse and continually growing, with a large integrated network of legacy cyber technologies. This presents a substantial and diverse surface area for cyber enabled attack to disrupt military operations.

Being able to accelerate next generation hardware and software technologies to phase out the cyber vulnerabilities within current computer networks is vital in order to reduce defence exposure to cyber attack.

So, the Defence and Security Accelerator (DASA) is pleased to launch a new Innovation Focus Area (IFA) called Reducing the Cyber Attack Surface, which aims to develop technologies that reduce the opportunity for cyber attacks on Ministry of Defence (MOD) systems and platforms.

This IFA is being run on behalf of Defence Science and Technology laboratory (DSTL) and Defence Science and Technology (DST) and seeks proposals that enable greater confidence and a level of assurance in military systems against cyber-enabled attack.

Can you help? Read the competition document now and submit your idea.

How much funding is available?

DASA expects to fund proposals within Technical Readiness Level 4 – 7 (TRLs) up to £300K for a 9 month contract. Proposed technologies should demonstrate by providing a roadmap describing how they would achieve a technical demonstrator by end of Financial Year 2023 if further funding was made available.

Key dates

Cycle 1 of the Reducing the Cyber Attack Surface IFA is open now, and it will close on 20 October 2021 at midday BST. Cycle 2 will run from 20 October 2021 to 05 January 2022.

A new generation of cyber resistant hardware and software

The MOD is interested in identifying and accelerating next generation hardware and software technologies to reduce the vulnerabilities within current and future computer networks and systems, focusing particularly on operational technologies.

We are looking for technologies that:

- intelligently apply technologies that significantly reduce the opportunity for cyber attack
- effectively raise the barrier to entry for adversaries and providing greater confidence and a level of assurance against cyber-enabled attack
- are novel and applicable across a whole “class” of attack surface rather than solutions tailored to a specific threat

Read the full competition document for more on what technologies we are looking for

Key challenges

DASA is seeking proposals that are applicable across a whole “class” of attack.

We are not seeking solutions that:

- offer demonstrations of off-the-shelf products requiring no experimental development (unless applied in a novel way to the challenge)
- offer no real prospect of integration into defence and security capabilities
- offer no real prospect of out-competing existing technological solutions

Submit a proposal!

The closing date for proposals of this IFA is 20 October 2021 at midday BST. A second cycle will run from 20 October 2021 to 05 January 2022. Click here for the full scope in the competition document and submit a proposal.

See DASA’s other cyber security IFA

You might also be interested in another cyber security IFA we are running called Autonomous Cyber Defence for Military Systems. This IFA seeks proposals that will develop autonomous cyber defence agents to protect military networks and systems.