ESRC Call:

ISCF Digital Security by Design Social Sciences Hub+

Summary

The Digital Security by Design Challenge, (DSbD) supported through the UK Government's Industrial Strategy Challenge Fund (ISCF), aims to overcome existing market failures and radically update the foundation of the insecure digital computing infrastructure that currently underpins the global economy.

Through leveraging the capability hardware concepts and approaches of the CHERI (Capability Hardware Enhanced RISC Instructions) program, a consortium led by ARM seeks to increase digital security through the development of a prototype solution based on ARM architecture. The scope of the broader challenge includes implementation, verification and proof of an updated hardware architecture, development of the software and system development tools that will run on it, and demonstration in at least two industry domains.

As the security landscape is inherently multi-dimensional, including cognitive, physical and virtual aspects – **this call will seek to understand the behavioural and adoption challenges in this area, working to define what it means to be secure, and insights into how to encourage businesses and society to move beyond management of risk to the adoption of secure practices.**

ESRC, on behalf of UKRI's ISCF are inviting applications from teams or consortia to lead the Digital Security by Design Social Hub+. This is to be a social sciences-focused Hub+ model. This consists of a central leadership team which will have with an allocated research budget to fund projects aligned with the DSbD programme. Funding is available of up to £3 million (80% FEC UKRI contribution for the main hub, and 100% FEC for the devolved research budget) until 31 March 2024. The Hub+ is expected to support and develop research and collaboration networks across the broader digital security landscape that address specific objectives within the scope of the Digital Security by Design challenge.

Applicant teams should submit **expressions of interest** to lead and manage the network by **15 November 2019**, with **outline bids** to follow by **12 December 2019.** A specially convened panel will review the outline submissions and invite a selection to submit a full proposal in January 2020, after which initial comments will be provided on the proposal in advance of an interview panel in May 2020. We expect to confirm the award week of 8 June 2020, and the network must start by the **7th September 2020**.

Background and scope

This Call forms one part of the wider ISCF Digital Security by Design challenge (https://www.ukri.org/innovation/industrial-strategy-challenge-fund/digital-security-by-design/). The DSbD Challenge is focussed on supporting both academic and industry research and development to enable the creation and potential adoption of a new technology platform protected with additional hardware-level capabilities.

To understand the technical scope of the proposed changes that will ensue as a result of the creation of the new technology platform, ARM and the University of Cambridge have published a technical descriptive article https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/cheri-faq.html

Future DSbD calls are expected to request business-led collaborative research and development proposals later in 2020, along with industry demonstrator projects funded through Innovate UK in 2022. The demonstrator projects, starting in 2022, will be required to articulate the economic benefit through the adoption of the new technology into a commercial environment and any mechanisms they require to overcome barriers to adoption, thus also requiring tight alignment with the Hub+.

The objectives of the Social Sciences Hub+ will be create a network that funds relevant research projects and links with the other investments made under the ISCF Digital Security by Design challenge. The Hub+ is expected to engage with the research base, businesses across the computer hardware and software sectors, security-focused industry users, and wider stakeholders such as national and local policy makers, industry bodies and the third sector

The Hub+ is expected to proactively engage with the other aspects of the Digital Security by Design challenge. It is anticipated the Hub+ will develop strong links and collaborations with the Demonstrators. Proposals under this call should describe plans for interaction, with the other activities funded, and facilitating discussions around the insights and findings from the funded projects.

The Hub+ is also expected to manage the community it creates including the network and communication activities. It is anticipated this will consist of the projects funded by the Hub+ and the activities across the ISCF DSbD challenge who will have a direct interest in the research of the Hub+ (such as the broader DSbD funded projects led by EPSRC and the technology platform arm-led consortium (comprising ARM, Linaro, university of Cambridge, university of Edinburgh)).

In addition to Hub+ events as determined by the successful team, the Hub+ will be expected to coordinate with the UKRI Programme team in the development and delivery of 2 events a year. These cross-programme workshops are expected to focus on technical, social and economic research outputs and how they can inform the development of the implementation of secure hardware technologies. To ensure this meets the programme aims it is expected the Hub+ will work closely with the UKRI DSbD Programme team in the delivery of the events.

Call details

We are commissioning an interdisciplinary Social Sciences Hub+ which is to have a dual responsibility:

- Create, build and manage the community of DSbD Hub+ participants
- Address both immediate and arising social and economic questions relevant to DSbD both directly and indirectly through a portfolio of devolved funded small team projects.

The following are 4 key topics the Hub+ must address. Each heading includes examples and potential questions – applicants are welcome to highlight additional areas that need to be addressed. Proposals must demonstrate a clear understanding of the challenges for each of the 4 key topics:

- Routes to adoption – barriers for business:
    - What makes businesses and public communities adopt new higher security practices, as opposed to following existing standards and best practices
    - What benefits can be achieved through early adoption of secure hardware? How can these be achieved?
    - What security costs, benefit perceptions and risk readiness levels influence routes to adoption?
    - Which challenges in identifying, meeting and managing real and perceived skills gaps form barriers for business, and in what way may they be surmounted?
    - How can secure hardware be integrated into existing business systems and secure working practices?
    - What shift in norms are needed to adopt secure practices?
- Routes to adoption – business and society readiness levels:
    - How do secure technology behaviours manifest along the consumer chain?
    - To what extent is future-proofing of readiness perceptions influencing readiness levels?
    - What attitudes to security exist in the software community, and how may they influence readiness levels or adoption of secure hardware?
    - In what ways does technology diffusion and differential security risks influence adoption pathways?
- Regulatory challenges and opportunities – barriers and enablers:
    - What are the policy/regulatory implications of improved computer hardware security – are there policy barriers to adoption or opportunities to accelerate adoption?
    - To what extent does the regulatory environment affect the increased adoption of hardware security?
- Social, cultural and commercial sector differences:
    - What perceptions of security and its meaning exist in commercial contexts?
    - What are the effects of risk readiness and technology diffusion along the consumer chain? What are the challenges and solutions to secure behaviours in different communities?

- What social and cultural attitudes to digital security exist, and how may they influence secure behaviours?
- To what extent do social networks and social media influence secure behaviour?
- To what extent can the economic benefits and disbenefits of security (real versus perceived) be effectively quantified?

The Hub+ design and objectives will need to fit within the overall vision and objectives for the ISCF Digital Security by Design challenge. The funded Hub+ will be required to complete a quarterly report for the UKRI team on the Hub+ operations and will include details for each of the funded projects, including progress and workplan updates, spend and objective tracking and financial reporting. This will be in addition to the annual ResearchFish submission and is required as part of monitoring and reporting on this ISCF funded investment.

Expectations

The Hub+ will:

- Enable a demonstrable understanding of the implications of security on business and society and the broader landscape challenges for the current cyber-security community
- Enable ongoing engagement with other funded DSbD activities to understand their challenges and new research and engagement opportunities for the Hub+
- Enable an active and demonstrable focus on impact within commercial environments
- Enable the development of new and inclusive collaboration networks across the DSbD programme through tailored activities such the bi-annual event, additional meetings and interactive fora. The Hub+ should also enable communication activities that proactively reach out to a wide range of academic disciplines, industrial partners and other external stakeholders. Appropriate support to manage this will need to be accounted for. The successful Hub+ will be expected to draw up a full communication and engagement plan within 3 months of the grant start date.
- Scope and publish competitions for proposals, design appropriate peer review processes in order to distribute funding beyond the core applicant team. The balance of activity funded in the 4 key topics highlighted should be proposed and justified by the applicants.
- Have in place an appropriate management team and risk management approach and suitable governance to ensure that competitions are run in a fair and transparent manner.
- Be expected to engage with the UKRI governance, monitoring and evaluation officer from the programme team and will need to ensure appropriate resources for this are in place.
- Provide a detailed workplan covering activities, events, communications, milestone objectives and associated channels of delivery.

- Proposals must evidence they have the appropriate mechanisms to allocate funding to researchers and outline the expected budget for this work.

Outcomes:

- Enhanced knowledge and understanding of the current landscape across the disciplines and sectors relevant to this challenge and inclusion of the best existing knowledge from wherever it is across the UK
- Funds distributed which will enable the development of excellent, impact-focused research and innovation
- Establishment of a multidisciplinary community including academia, industry and other stakeholders that will identify and tackle the challenges associated with the ISCF Digital Security by Design programme
- Appropriate links established both nationally and internationally in order to ensure UK research remains globally competitive.
- Informing the broader evidence base and influencing discussions around the 4 key topics. This is anticipated to include:
    - Routes to adoption – barriers for business
    - Routes to adoption – business and society readiness levels:
    - Regulatory challenges and opportunities – barriers and enablers
    - Social, cultural and commercial sector differences

Structure and resources

We are inviting applications for leadership teams to lead **a single Hub+** until March 2024**,** with funding available of up to £3 million split between Hub+ costs and small project funding (80% FEC for Hub+, 100% FEC for small project funding).

We encourage the project team or consortium to extend over more than one research organisation. It is expected this will be justified in the case for support.

We will be not be asking for full costings until the outline stage. Applicants should note that the spend profile of this grant will reflect our expectation that significant work is undertaken in the first six months to bring the community together, including a substantial launch or initial networking event and an initial round of small projects. Applicants should also note that the intended ratio of Hub+ and small project funding should form part of the expression of interest.

Total funding will cover:

- the administration and management of the Hub+ and associated knowledge exchange programme, including employment of a network co-ordinator
- the commissioning of a series of small projects, as outlined above – a budget which would be held by the network lead and allocated to the wider network on the basis of fair and transparent procedures and criteria
- knowledge exchange activities to bring together DSbD investments, the research base, key businesses and other stakeholders

The applicant teams successful at the expressions of interest stage will be asked to justify in their full proposal what they believe to be the appropriate division of the available funds between the above activities. These should ensure that funds genuinely enable new work rather than going towards existing activities and give due consideration to issues of diversity and capacity-building.

We strongly encourage project partners who are able to provide in kind or cash contributions to this network to increase the potential scale of its activities.

The small project fund should be delivered in line with ESRC eligibility requirements – the small projects must be from an eligible research organisation but collaboration with business and other stakeholders is encouraged. We will work with the successful applicant team at the full proposal stage to ensure that these limitations on funding do not unduly restrict full business and other partners' participation in the network.

The funding for this Hub+ will be provided as a single grant to the host research organisation where the principal investigator is located.

Monitoring, investment management and evaluation

As with all ISCF activities, the UKRI team will have an active investment management relationship with this Hub+. The ISCF challenge director will have the right to terminate activities that are not delivering on objectives, and all challenge activities will be evaluated by a challenge-level board.

Leadership team

We require the Hub+ leadership team (Principal and Co Investigators) to collectively contribute a significant proportion of their time to the overall leadership and direction of the Hub+. The expression of interest should provide initial indications of the management structure, which will be further described in the proposal. We expect that the full team including the network coordinator and/or project manager responsibilities for the duration of the network will be outlined within the full proposal.

There is no formal restriction on who may constitute the leadership team, beyond the need for the PI to be an academic at an organisation eligible for funding by ESRC. Constraints on the involvement of non-academic investigators will be in place in line with ESRC's policy, available here: https://esrc.ukri.org/files/funding/guidance-for-applicants/inclusion-of-uk-business-third-sector-or-government-body-co-investigators-on-esrc-proposals/

For the expressions of interest stage, the Hub+ leadership team should be structured with a principal investigator and 1 to 3 co-investigators who can be drawn from UK affiliated research organisations (including overseas) and non-academic organisations including businesses.

The investigators named in the expression of interest are expected to constitute the core of the leadership team. You should not add the names of potential network members who are not intending to lead the network to the list of investigators.

The team should be able to engage with a range of disciplines including but not limited to the engineering and physical sciences, the breadth of social sciences, security and defence,

and communications. The team should also be able to engage with businesses across the commercial sectors covered by the Digital Security by Design challenge.

All investigators must be justified as adding different expertise, skills and background to the leadership team and must be an active part of the core team running the network plus.

The team should:

- Lead the preparation of an outline Hub+ proposal to be submitted no later than 12 December 2019 and if invited, a full Hub+ proposal to be submitted no later than 27 March 20202

Publication and Intellectual Property Rights (IPR)
Publication and IPR will be handled in accordance with normal ESRC guidelines outlined in the Research Funding Guide (www.esrc.ac.uk/rfg). All research findings should be made freely and openly available. RCUK policy statements on IPR, impact and knowledge exchange are available at www.rcuk.ac.uk/ke/policies/

How to apply

Initial expressions of interest (EoI) to state your interest in applying for this call should be submitted to dsbd@esrc.ukri.org, to be followed by an outline proposal submitted through Je-S. Please note that the EoI is NOT for any assessment purpose. The EoI is to help ESRC plan the peer review and the panel arrangements.

Applicants should not await a response from the funders following the EoI submission, but simply continue with the development of their outline proposals, submitted through Je-S.

A) The outline proposal submission
The outline proposal must be no longer than 5 pages and evidence:

1. Leadership team
2. Proposed Hub+ structure (and associated funding structure)
    a. Area/topic coverage
    b. Outline approach to project funding across DSbD scope
3. Approach to developing and communicating with the Hub+ community
4. Justification of resources required to undertake the research project, indicating why the resources are needed and taking into account the division of resources between Hub+ operational expenditure and the small project funding pot.

Two page summary CVs for the PI and co-applicants may also be attached, as well as a note of support with the name of a senior colleague – such as a pro-vice chancellor or head of the research office – who can confirm the host organisation endorsement for this application. This will evidence the host research organisation's endorsement for this application.

Outline submissions must be submitted through the Joint Electronic Submission (Je-S) system. Je-S is the electronic submission system which is used by all Research Councils to provide a common electronic system that supports research administration. More detailed information can be found at https://je-s.rcuk.ac.uk/.

B) The full submission proposal

Applicants invited to submit a full submission, in addition to the standard documents, should expect to also include a single attachment with the headings and word limits below:

1. **Hub+ Ethos and Strategy (500 words)**– What goals, strategy and direction are you envisioning for the Hub+? How will you seek to engage the diverse community of DSbD participants and associated stakeholders for effective knowledge exchange? How are you giving appropriate consideration of diversity, ethics and responsible innovation?
2. **Impact of the Hub+ (500 words)** What do you think the contribution of the Hub+ will be to the ISCF Digital Security by Design challenge, other ISCF challenges, the wider research and business community, and other stakeholders, and the pathways to achieve such impact?
3. **Managing a devolved budget (500 words).** Provide evidence of previous experience managing a budget that is subsequently devolved (e.g. a longer, large grant or project).
    - How will you ensure the budget is devolved to other parties using a process that is fair and transparent? How will you invite and assess proposals, make funding decisions, then monitor projects after award?
    - How will you ensure that the budget is distributed to meet the needs of the community and ISCF stakeholders? How will you ensure the funded projects are focused and responsive?
4. **Hub-Network Building (500 words)**. Provide evidence of your experience of bringing together a distributed and diverse community of people, making sure you describe the outcomes of the activity. Please highlight where this involved a range of academic disciplines and/or business sectors.
    - Indicate how you intend to attract different disciplines into this network?
    - How do you intend to attract non-academic (including business) members and encourage them to devote time to engaging in your network?
    - How do you intend to effectively communicate the findings of the Hub+ and engender key knowledge exchange practices?
5. **Management of the Hub+ (500 words).** Provide an example of large-scale activities where project management of large groups of stakeholders has been required; this could be a complex activity that you currently lead or have led in the past.
    - Briefly describe the governance and model you propose for managing this Hub+? What staff resource will you recruit? What resources will the host organisation provide in support of the Hub+?
6. **Institutional Support -** Please provide a 1-page signed letter outlining support the institution will provide from an appropriate authority, e.g. PVC or Head of Research Office (not Head of Department)
7. **Project partners –** where businesses or other organisations have agreed to be project partners on the Hub+, this must be highlighted in the appropriate area of the

Je-S form and must outline matched/in kind funding or other means of support. Please attach letters indicating the project partner support with associated contributions.

8. In addition to these headings, applications should note the justification for resources should specifically account to the team's costs expected in managing the communications and engagement activities highlighted. Note for the biannual events the Hub+ will not be required to cover the costs of the venue/catering or the expenses of attendees.

Assessment

An independent assessment panel comprising of academics, business representatives and other stakeholders will assess outline submissions against the following criteria. An expanded version of these criteria will be used in the assessment of the full proposal, and provided to the shortlisted candidates:

1. Quality of the proposal to manage the research and impact focussed activities proposed and fit to the aims of the Digital Security by Design challenge
2. Quality and experience of the leadership and Hub+ team
3. Quality of the impact plan
4. Justification of resources
5. How a network will be developed and managed, including appropriate consideration of diversity, ethics and responsible innovation
6. Clarity by which the programme will be delivered, including management of the project funding budget

Commissioning timetable

- Call opens 15th October 2019
- Deadline for Expressions of Interest 15 November 2019
- Deadline for Outline Proposal 12 December 2019
- Invitation to submit Full Bid 30 January 2020
- Deadline for full proposal 26 March 2020
- PI responses to Peer review – 11 May 2020
- Interview panel 28 May 2020
- Confirm Award Week of 8 June
- Start no later than 8 September 2020

Contacts

- Case officer: Charlotte Ashbrooke
  Email: dsbd@esrc.ukri.org
  Telephone: 07522 218491