ISCF Digital Security by Design Research Projects

Call type: Invitation for proposals

Closing date: 7 January 2020, 16:00

Funding Available: Up to £8M to support 6 - 9 research projects to cover all three objectives within the scope of this Call.

How to apply: Full proposal

Assessment Process: Full proposals will undergo postal peer review, followed by panel (if reviews are sufficiently supportive), resulting in a rank ordered list. Final funding decisions will be made using a portfolio approach to ensure coverage both across, and within, the three objectives within the scope of the call.

Key Dates:

Activity	**Date**
Call published	26 September 2019
Deadline for Full Proposals	7 January 2020
Prioritisation panel	April 2020
Funding decision	April 2020
Grant start date (fixed start date)	1 June 2020

Additional information: Grant durations accepted for 3 – 4 years (N.B. **project end dates must be no later than 31 March 2024**). Applicants to cost in resources to their proposals for attendance at a biannual event, for dissemination and networking among all projects and with industrial partners.

Contacts:

Marianne Rolph, 01793 444002, Marianne.Rolph@epsrc.ukri.org

Rhys Perry, 01793 444466, Rhys.Perry@epsrc.ukri.org

ISCF Digital Security by Design Research Projects

Call type: Invitation for proposals

Closing date: 7 January 2020, 16:00

Related themes: ICT, Digital Economy

Contents of this call document

Summary

The Industrial Strategy Challenge Fund (ISCF) Digital Security by Design challenge (https://www.ukri.org/innovation/industrial-strategy-challenge-fund/digital-security-by-design/) is executing a mission to increase the protection of software in the light of increased cyber attack against various class of software vulnerabilities, through additional hardware protection capabilities architected around the containment of pointers, and the privilege by which regions of fine grain data can be accessed.

Leveraging the **Capability Hardware** (https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/dsbd.html) concepts and approaches investigated by the CHERI program (led by the University of Cambridge), a consortium led by Arm is investigating a prototype silicon-based solution based on Arm AArch64 architecture. This prototype solution will be made

openly available to academics and businesses across the UK, so as to provide early access, evaluation, and the opportunity to feed back on the proposed major change to the instruction set architecture of a processor, while investigating the broader impact to various aspects of computer science and ICT in general.

EPSRC, on behalf of the Industrial Strategy Challenge Fund (ISCF), would like to commit up to £8M (at 80% FEC) to support academic research projects from **across the broader research landscape** that address specific objectives within the scope of the Digital Security by Design challenge. The aim is to support innovative research projects that will help to move the technology beyond the state of the art, moving Capability Hardware concepts and use forward, without duplicating or conflicting with the existing CHERI research. Applications for full proposals are sought from project teams based at Research Organisations in the UK who are eligible to receive EPSRC funding.

To understand the 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 descriptive article (https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201909-cheri-intro-dsdb.pdf). Initial models and a formal specification using the Arm Architecture Specification Language (https://alastairreid.github.io/specification_languages/) along with a virtual model of the platform (https://www.arm.com/products/development-tools/simulation/fixed-virtual-platforms) will be made available to successful applicants around the start of the project (June 2020). A silicon based prototype platform will be available one year later (c. June 2021), in which a recent superscalar ARM Cortex-A class multicore processor will be enabled with Capability Hardware. This device will be mounted on a development board supporting display, networking and peripheral extension with a Linux Kernel, and in the first instance, an Android user space and associated development tools.

A workshop (**or** virtual workshop/webinar) for potential applicants will be held in November 2019 to discuss further details relevant to this Call and to enable the development of interactions and potential collaborations.

Projects that are funded under this Call will need to fit within the overall vision and objectives for the ISCF Digital Security by Design challenge (https://www.ukri.org/innovation/industrial-strategy-challenge-fund/digital-security-by-design/). Advice will be sought from the Digital Security by Design External Advisory Group to provide guidance on the overall direction of research across all funded projects within the challenge and the complementarity to achieving the vision of the challenge.

Funded projects will be required to report on progress and to provide financial reports, in addition to the annual ResearchFish submission, as part of monitoring and reporting arrangements on this ISCF-funded investment.

Project partners (industrial partners and/or academic collaborators) are encouraged as part of this call, where this is appropriate for the research being proposed.

Successful applicants will be required to attend a biannual event of all stakeholders and collaborators within the ISCF Digital Security by Design challenge, for dissemination and networking purposes. Project partners and

collaborators for each funded project are also encouraged to attend these events. The aim of this is to share developments across the various challenge objectives to feed back into the overall ISCF Challenge. In addition, proposals under this Call should describe future plans for interaction with the Digital Security by Design Social Sciences Hub+ to discuss implications arising from the technical developments and factors that may affect the potential routes to adoption for the new technology (see the ESRC Call announcement here: https://esrc.ukri.org/funding/funding-opportunities/iscf-digital-security-by-design-social-science-hub/). It is expected that representatives of all projects funded by the ISCF challenge, including from the Social Sciences Hub+ and the Arm-led consortium (comprising Arm, Linaro, University of Cambridge, University of Edinburgh), will attend the biannual events to enable discussion of research outputs and how this informs the future development of technologies for a secure hardware technology platform.

Background

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/), which is focussed on supporting both academic and industry research to enable the creation and potential adoption of a new technology platform with additional hardware protection capabilities.

The objectives of this Call are to support academic research for further investigation relating to the broader impact and opportunities of Capability Hardware and the prototype technology platform that is being created by the Arm-led consortium.

Applications are invited for proposals that meet **one of the following objectives only**: 1) Capability enabled hardware proof and software verification; 2) Impact on system software and libraries; 3) Future implications of Capability Hardware.

Please note that under each objective below, a number of example research questions have been provided. These questions are only given as examples in each case and are not exhaustive or exclusive. This Call is open broadly to **new approaches and novel research projects** that could meet any of the three objective areas, including ideas and approaches that have not specifically been listed as examples in the Call document.

Objective 1: Capability enabled hardware proof and software verification

Despite the historical best efforts of hardware to execute software as expected by software, it became impossible to reason on its completeness given the lack of formal specification of the hardware architecture and the complexity of any specific design. Various advances are being made with respect to the formal proof of hardware resulting in the increasing accuracy and formal specification of the hardware architecture. However, linking the work of hardware proof with software reasoning and verification **in the context of Capability Hardware** needs significant research to find a methodology by which the final intent of an application can be understood and verified, including side-channel effect in the

hardware, and the limited specification for data encapsulation and privilege in software. The aim is to fund research across this objective including, but **not exclusively**, summarised below:

- Through the introduction of Capability enabled Hardware, what tools or techniques can be applied in limiting and/or identifying leakage of information, including but not limited to, containment analysis and various forms of information flow within software?

- Can (and if so, how can) the formal specifications of hardware be extended to include microarchitectural artefacts beyond the architectural specification often responsible for side-channel or inference-based information leakage?

- How can a system dynamically learn and monitor the correct operation of a platform's intent, to provide necessary information to mitigate inappropriate operations potentially identified as a divergence from a runtime specification or a learning associated with historic operation?

- Given a formal executable hardware architectural specification, how can we increase the capabilities and understanding of formal method and proof with respect to the expected execution of software, its proof and verification?

These questions are only given as examples; this objective is open for ideas and approaches that have not specifically been listed here.

Objective 2: Impact on system software and libraries

Today's platform capable computers contain software and its data within a single virtual address space, which is often shared with the operating system (OS) and isolated solely by a processor's context. As such, the injection of code following a software fault can cause the leakage of information from the application, or loss of control of all software if it occurs in the OS context. Today's computers apply no distinction between the execution of expected and unexpected code sequences.

There are various implications and potential solutions to **extending current software** and "end-2-end" security schemes to include the movement of data with fine grain protection and inherited rights. For example, how to extend cryptography frameworks to extend the protection of information from the point of encryption to the point of use in an application, through the application of Capability Hardware.

Existing platforms support various software and hardware assisted mechanisms to encapsulate the various states of an application as an aid towards increasing security or limiting visibility of data. Whether this is through a managed runtime, a trusted execution engine, the interpretation and translation of binaries, or larger grain hardware protection schemes, the introduction of fine grain data containerisation and access privilege will bring new opportunities and new threats. Investigations are required to understand these implications and to propose how existing system software and libraries will adapt to such new

hardware mechanisms. The aim is to fund research across this objective including, but **not exclusively**, summarised below:

- How can existing managed runtimes, high-level languages or systems leveraging binary translation of code benefit from the introduction of Capability enabled Hardware and improve the security of applications and services?

- What are the impacts and opportunities from Capability Hardware to increase the security between and within platforms, using a trusted execution engine (TEE) or other virtualization technologies? How will the delivery or use of such technologies change?

- How can the increased security provided by Capability Hardware be extended robustly to operate security over a distributed system?

These questions are only given as examples; this objective is open for ideas and approaches that have not specifically been listed here.

Objective 3: Future implications of Capability Hardware

When virtual memory was first introduced, the ways in which this coarse grain memory partitioning and access privilege would be used was unknown. Although various characteristics of how virtual memory is managed by a processor has evolved, the fundamental concepts remain unchanged. Given the wider challenge objective to introduce fine grain compartmentalisation and inherited privilege capabilities to a processor, the **future implications** and potential use cases are unknown. The aim of this objective is to fund early stage research into the longer term implications of the new memory projection paradigm. **Potential** questions include:

- Today's operating systems use virtual memory for the protection of code and data, process isolation and the associated scheduling mechanisms. Since a Capability enabled processor offers stronger and more fine grained protection than current systems, what might the implications and opportunities be when reconsidering these requirements of an operating system?

- What are the implications and opportunities of Capability Hardware existing in the central processing unit (CPU) on other hardware devices such as direct memory access (DMA) devices and processors of a digital system and their associated software stacks?

These questions are only given as examples; this objective is open for ideas and approaches that have not specifically been listed here.

The research to be funded under this Call relates primarily to the ICT and Digital Economy portfolios in EPSRC. For more information about EPSRC's portfolio and strategies, see our website: https://epsrc.ukri.org/research/ourportfolio/

This Call forms part of the wider Digital Security by Design challenge, which will also include activities and competitions led by Innovate UK and the Economic and

Social Research Council (ESRC). ESRC will be launching a call for a Digital Security by Design Social Sciences Hub+ in Autumn 2019, looking specifically at issues around routes to adoption for the new technology platform. Projects that are funded through the EPSRC call will be encouraged to interact with the Social Sciences Hub+ to share knowledge and ideas, in order to understand and enable potential routes to adoption.

Funding available

Up to £8M is available, to be allocated across the three objectives. It is anticipated that 6 - 9 projects will be funded in total. These are expected to have a duration of between 3 and 4 years (with **project end dates no later than 31 March 2024**).

Successful applicants will be expected to attend a biannual one day event in the UK of all challenge stakeholders and collaborators. Applicants should cost in resources to their proposals for attendance at these events.

Equality, Diversity and Inclusion

The long term strength of the UK research base depends on harnessing all the available talent. EPSRC expects that equality and diversity is embedded at all levels and in all aspects of research practice and funding policy. We are committed to supporting the research community, offering a range of flexible options which allow applicants to design a package that fits their research goals, career and personal circumstances. This includes career breaks, support for people with caring responsibilities, flexible working and alternative working patterns. With this in mind, we welcome applications from academics who job share, have a part-time contract, or need flexible working arrangements.

Peer review is central to EPSRC funding decisions; we require expert advice and robust decision making processes for all EPSRC funding initiatives. We are committed to ensuring that fairness is fully reflected in all our funding processes by advancing policy which supports equality, diversity and inclusion. Please see our Equality and Diversity webpages https://epsrc.ukri.org/funding/equalitydiversity/ for further information.

Guidance on Journal-based metrics

As part of our commitment to support the recommendations and principles set out by the San Francisco Declaration on Research Assessment (DORA; https://sfdora.org/read/), UKRI reviewers and panel members are advised not to use journal-based metrics, such as journal impact factors, as a surrogate measure of the quality of individual research articles, to assess an investigator's contributions, or to make funding decisions.

The content of a paper is more important than publication metrics, or the identity of the journal, in which it was published, especially for early-stage researchers. Reviewers and panel members are encouraged to consider the value and impact of all research outputs (including datasets, software, inventions, patents, preprints, other commercial activities, etc.) in addition to research publications. We advise our peer reviewers and panel members to consider a broad range of

impact measures including qualitative indicators of research impact, such as influence on policy and practice.

Equipment

Equipment over £10,000 in value (inc. vat) is not available through this call. Smaller items of equipment (individually under £10,000) should be in the Directly Incurred - Other Costs heading.

For more information on equipment funding, please see: https://epsrc.ukri.org/research/facilities/equipment/

The proposal case for support must include an indication as to **how many (if any) instances of the model and/or development platform will be required** for the proposed research. Reasonable and appropriately justified requests will be provided for use by successful applicants at no cost.

Eligibility

Any single investigator is only permitted to appear on **one application**, either as a PI or Co-I.

If more than one application is submitted containing a single investigator, the investigator will be asked to withdraw from being on one of the two applications (if a Co-I), or alternatively to withdraw an entire proposal (if listed as the PI).

Please ensure sufficient time to create Je-S accounts for investigators who do not currently have one.

For information on the eligibility of organisations and individuals to receive EPSRC funding, see the EPSRC Funding Guide: https://epsrc.ukri.org/funding/applicationprocess/fundingguide/

A list of eligible organisations is provided at: https://www.ukri.org/funding/how-to-apply/eligibility/

How to apply

Submitting an application

You should prepare and submit your proposal using the Research Councils' Joint electronic Submission (Je-S) System (https://je-s.rcuk.ac.uk/).

When adding a new proposal, you should select:

- Council 'EPSRC'
- Document type 'Standard Proposal'
- Scheme 'Standard'
- On the Project Details page you should select the 'ISCF Digital Security by Design Research Projects' call.

Note that clicking 'submit document' on your proposal form in Je-S initially submits the proposal to your host organisation's administration, not to EPSRC. Please allow sufficient time for your organisation's submission process between submitting your proposal to them and the call closing date. EPSRC must receive your application by **16:00 on 7 January 2020**.

Guidance on the types of support that may be sought and advice on the completion of the research proposal forms are given on the EPSRC website (https://epsrc.ukri.org/funding/applicationprocess/) which should be consulted when preparing all proposals.

Guidance on writing an application

Applicants are required to identify which one of the three Call objectives they are applying against in the proposal cover letter.

The following documents should be added as PDF attachments and submitted with the Je-S form:

- Case for support: should be up to eight pages in total, to include:
    - Two-page track record, which should detail the relevant expertise that each investigator will bring to the research
    - Six-page description of the proposed research focus and how this fits the aim and scope of the call. This should include a clear statement of the proposal's vision, and how each strand of activity complements this vision. Applicants should also include how the work proposed relates to **one** of the Call objectives **only** (detailing which one of the three objectives the proposed research relates to). Must also include an indication as to how many (if any) instances of the model and/or development platform will be required for the proposed research. (Reasonable and appropriately justified requests will be provided for use by successful applicants at no cost.)

- Pathways to Impact: should be up to two pages and is primarily for detailing the activities which will help develop the potential economic and societal impacts. Please detail how the proposed research project will be managed to engage users and/or beneficiaries and increase the likelihood of impacts. To also include description of future plans for interaction with the Digital Security by Design Social Sciences Hub+ (to be funded by ESRC). Please note the requirement to include funding for attending a biannual networking meeting of all projects with the wider stakeholders and collaborators for the ISCF Digital Security by Design challenge.
    - More details of the type of resources that can be requested through the Pathways to Impact can be found in the Funding Available section of this document. More information on preparing the impact plan and on impact can be found on the EPSRC website at: https://www.epsrc.ac.uk/funding/howtoapply/preparing/impactguidance/

- Justification of resources: should be up to two pages. This should be a narrative description of the need for the resources requested. Applicants are required to request resources for attendance at the biannual

networking events for all award holders and collaborators in the ISCF Digital Security by Design challenge.

- Work plan: should be up to one page. It is not expected that this will be a Gantt chart for the whole duration of the project, but should include a comprehensive plan for the start of the project (years 1-2) and then refer to the management strategy to give appropriate milestones for how and when important decisions on the direction of the remaining research will be taken.

Applicants should use the Ethical Information section on the Je-S form to demonstrate to peer reviewers that they have fully considered any ethical issues concerning the material they intend to use, the nature and choice, current public perceptions and attitudes towards the subject matter or research area. EPSRC will not fund a project if it believes that there are ethical concerns that have been overlooked or not appropriately accounted for. All relevant parts of the Ethical Information section must be completed. If the research will involve human participation or the use of animals covered by the Animals (Scientific Procedures) Act 1986 it is recommended that applicants pay particular attention to the guidance highlighted below. EPSRC reserves the right to reject applications prior to peer review if the Ethical Information sections are not completed correctly.

Further guidance on completing the Je-S form can be found at https://je-s.rcuk.ac.uk/Handbook/pages/GuidanceonCompletingaStandardG/EthicalInformation.htm. Other relevant guidance includes: EPSRC's policy on animal use in research (https://www.epsrc.ukri.org/about/standards/animalresearchpolicy/) and the Responsible Innovation Framework (https://epsrc.ukri.org/research/framework/).

Please note that on submission to EPSRC **all** non-PDF documents uploaded onto Je-S are converted to PDF, the use of non-standard fonts may result in errors or font conversion, which could affect the overall length of the document.

For advice on writing proposals see:
https://epsrc.ukri.org/funding/howtoapply/preparing/

User Engagement Strategy

For applicants submitting against Objective 1 (Capability enabled hardware proof and software verification) and Objective 3 (Future implications of Capability Hardware):

Successful applicants will be required to develop and execute a strategy for engaging with stakeholders, award holders and collaborators from across the broader ISCF Digital Security by Design community (including the ESRC-funded Digital Security by Design Social Sciences Hub+). Resources for this activity can be requested as part of the Pathways to Impact and must be justified in the application.

For applicants submitting against Objective 2 (Impact on software systems and libraries):

Successful applicants will be required to develop and execute a strategy for engaging with potential users of the research funded in the project. This strategy

should be reviewed and updated regularly as part of the formal management of the grant.

The strategy should cover:

- how and when potential users have been / will be identified;
- what form the engagement will take;
- what steps will be taken to ensure that outputs of the research are made available to potential users;
- suitable metrics for determining the success of the strategy in delivering value to users.

Successful applicants will also be required to develop and execute a strategy for engaging with stakeholders and collaborators from the broader ISCF Digital Security by Design community (including the ESRC-funded Digital Security by Design Social Sciences Hub+).

Resources for these activities can be requested as part of the Pathways to Impact and must be justified in the application.

Assessment

Assessment process

Assessment of proposals will take the form of: (1) postal peer review and (2) prioritisation panel.

Stage 1: Postal Peer Review

Proposals will be reviewed via postal peer review. In addition to the standard assessment criteria, reviewers will also be asked to consider the proposal according to the fit to call, i.e. the extent and degree of alignment between the proposed research and **one of** the objective areas identified within the scope of this Call. If a proposal receives sufficiently supportive reviewers' comments it will go forward to stage 2 of the assessment process. Please find more information about this standard assessment process here https://www.epsrc.ac.uk/funding/assessmentprocess/overview/

Stage 2: Prioritisation Panel

Proposals will be assessed and ranked by a panel using the assessment criteria provided below, taking into account the feedback from the reviewers and the response provided by the applicant. The panel will produce a prioritisation rank order of the proposals it has considered in order of merit, and will have taken all relevant criteria into account in doing so.

A portfolio approach will be taken for the final funding decisions to ensure that there is coverage both across, and within, all three objectives in the Call. The ISCF Challenge Director has oversight of the Digital Security by Design Challenge. Where there is any conflict of interest, or perceived conflict, decisions will be delegated as appropriate.

Assessment criteria

The following assessment criteria will be used to assess proposals submitted to this call:

Fit to call (Primary):

- **How well** (to what degree and extent) does the research proposed align with and address **one** of the following Call objective areas (as per the technical scope described within the 'Background' section of the Call document) –
    - 1) Capability enabled hardware proof and software verification
    - 2) Impact on system software and libraries
    - 3) Future implications of Capability Hardware.

Quality of research (Secondary Major):

- Novelty and timeliness
- Appropriateness of proposed methodology

National importance (Secondary):

- New activity that adds to, and aligns with, national activities in cyber- and digital-security research
- Responsible innovation has been considered and explored

Pathways to impact (Secondary):

- Relevance and appropriateness of any beneficiaries or collaborators
- Plans for dissemination and knowledge exchange
- Appropriate resources have been requested to support any required community building, responsible innovation and/or public engagement

Ability of applicant team to deliver the research (Secondary):

- Track record of the team
- Balance of skills of the project team and integration of different methodologies and approaches

Resources and management (Secondary):

- Effectiveness of the planning and resource management strategy, including: the planned approaches to the research beyond year 1-2, with appropriate indications and milestones for how and when important decisions on the direction of the remaining research will be taken.
- Appropriateness of resources requested.

Feedback

Feedback will consist of reviewers' reports and (if they are sufficiently supportive) the ranking position at the prioritisation panel, noting that final funding decisions will have been made using a portfolio approach to ensure coverage across, and within, the three Call objectives. The prioritisation panel may provide specific feedback to applicants if deemed necessary, but this will not be issued as standard.

Guidance for reviewers

Information about the EPSRC peer review process and guidance for reviewers can be found at: https://epsrc.ukri.org/funding/assessmentprocess/review/

Guidance for reviewing standard grants can be found here: https://epsrc.ukri.org/funding/assessmentprocess/review/formsandguidancenotes/standardgrants/

Please note the additional requirement to assess the fit to call as part of the review – comments relating to this criteria should be recorded within the '**Proposal Assessment**' box on the reviewer form. See the information contained under 'Assessment Criteria' above for further details.

Grant additional conditions (GACs)

Grants will be subject to the standard UK Research and Innovation grant conditions however the following additional grant conditions will be added to this call:

GAC 01 – Challenge Networking

Grant holders will be expected to attend a biannual UK based meeting of all projects, stakeholders and collaborators that form part of the Industrial Strategy Challenge Fund (ISCF) Digital Security by Design Challenge. Funds for attendance must be allocated from within the grant award for this purpose.

GAC 02 - Start date of the Grant

Notwithstanding RGC 5.2 Starting Procedures, this grant has a fixed start date of 1 June 2020 – no slippage of this date will be permitted. Expenditure may be incurred prior to the start of the grant and be subsequently charged to the grant, provided that it does not precede the date of the offer letter.

GAC 03 - Publicity and Branding

In addition to RGC 12.4 Publication and Acknowledgement of Support, the Grant Holder must make reference to ISCF and UKRI funding and include the ISCF and UKRI logos and relevant branding on all online or printed materials (including press releases, posters, exhibition materials and other publications) related to activities funded by this grant.

In future, once a brand name for the Capability Hardware has been identified, the Grant Holder must also make reference to this brand name, particularly in any research publications or future funding applications that build directly upon the work funded in this award.

GAC 04 - Governance

Further to RGC 7 Monitoring, this grant is subject to the framework principles of the Industrial Strategy Challenge Fund (ISCF) and will be expected to work

alongside other grants and governance structures under this scheme where appropriate.

EPSRC may nominate a member of UKRI staff (The Project Officer) who will be your primary point of contact. The Project Officer will ensure that the project is being run in accordance with the terms and conditions and in line with financial due diligence. The Project Officer(s) should have access to all documentation of Governance and Reporting bodies, in so far as it relates to the administration and application of the grant. As funding administrators, all UKRI staff have agreed to maintain the confidentiality required by all parties involved in EPSRC funded research.

GAC 05 - ISCF Challenge Director

This grant is supported through the Industrial Strategy Challenge Fund (ISCF) which is led by a UKRI-appointed ISCF Challenge Director. In accepting this award, the Principal Investigator acknowledges the need for the Challenge Director to have control over the Challenge to ensure that the work supported under this grant contributes to the overall delivery of the Challenge. Whilst the Principal Investigator is expected to take advice from the Challenge Director to steer the research towards meeting the aims of the challenge, the PI still retains control of the project funds for the duration of the project with advice from the Management Team and Advisory Group.

GAC 06 - Review

In addition to the requirements set out in standard UKRI grant conditions RGC 7.4 Research Monitoring and Evaluation, 7.5 Disclosure and Inspection, EPSRC reserve the right to instigate a review of all or part of the grant at any stage during the lifetime of the award as well as after the grant has finished. EPSRC will give the Grant Holder due notice of the date of any review and will provide details of the Terms of Reference and documentation required.

GAC 07 - Reporting

In addition to the requirements set out in the standard UKRI grant condition RGC 7.4.3, the Grant Holder is responsible for providing progress reports against non-financial performance metrics. A detailed list of performance metrics and instructions for reporting will be agreed with the Grant Holder upon commencement of the grant. UKRI reserves the right to ask for additional information as needed to meet overall reporting requirements for ISCF.

Moving forward

Submissions to this call will count towards the Repeatedly Unsuccessful Applicants Policy. Further information about the policy can be found at: https://epsrc.ukri.org/funding/howtoapply/basics/resubpol/rua/

Key dates

Activity	Date*
Call published	26 September 2019
Deadline for Full Proposals	7 January 2020
Prioritisation panel	April 2020
Funding decision	April 2020
Grant start date (fixed start date)	1 June 2020

*EPSRC aims to adhere to the key dates as published, however there may be exceptions where a sift, prioritisation or interview meeting may have to change due to panel member availability.

Contacts

Marianne Rolph, 01793 444002, Marianne.Rolph@epsrc.ukri.org

Rhys Perry, 01793 444466, Rhys.Perry@epsrc.ukri.org

JeS helpdesk (for any questions relating to using Je-S): 01793 444164, JeSHelp@je-s.ukri.org

Please ensure you contact your university research office for advice on internal processes relating to proposal submission to EPSRC. Please allow enough time before the closing date to enable submission. Proposals will not be accepted if received after the closing time and date.

Change log

Name	Date	Version	Change
Natasha Richardson	17 September 2019	1.0	
Natasha Richardson	26 September 2019	1.1	Inclusion of web link to 'Introduction to CHERI' article
Natasha Richardson	30 October 2019	1.2	Inclusion of web link to ESRC Call for Digital Security by Design Social Science Hub+
Natasha Richardson	08 January 2020	1.3	Change of Call contact details to Marianne Rolph

Appendices (includes Attachment Checklist and Fund Headings)

Je-S attachments Check List

Standard:

Attachment Type	Maximum Page length	Mandatory/Optional	Extra Guidance
Case for Support	Eight pages	M	Comprising up to two A4 sides for a track record, and six A4 sides describing proposed research and its context.
Pathways to Impact	Two pages	M	
Workplan	One page	M	
Justification for Resources	Two pages	M	
CVs	Two pages each	Not required (**except** for named and visiting researchers, and researcher co-investigators).	To be included for **named** and visiting researchers, and researcher co-investigators only.
Project Partner Letters of Support	No page limits	Required for any project partners named on the proposal form.	Must be included from all named project partners. Must be on headed paper, and be signed and dated within six months of the proposal submission date.
Letters of Support	No page limits	Not required	In exceptional circumstances a maximum of three letters can be submitted.
Equipment Quotes	No page limits	Not required	Equipment not permitted for this Call.

Equipment Business Case	Two pages each	Not required	Equipment not permitted for this Call.
Technical assessment	No page limit	Not required	
Proposal Cover Letter	No page limit	Required	The cover letter should be used to highlight any important information to EPSRC, including **which Call objective the proposal relates to**. This attachment type is not seen by reviewers or panel members.
Other attachment	No page limit	Not required	This can be used for a document that does not fit under any of the headings above. This attachment type is not seen by reviewers or panel members.

Please ensure you adhere to the above attachment requirements when submitting your proposal. Any missing, over length or unnecessary attachments may result in your proposal being rejected.