EPSRC
Engineering and Physical Sciences Research Council

Quick Reference

Please note that you must read the full Call document for guidance before submitting your proposal

Security for all in an AI enabled society

Call type: Invitation for proposals

Closing date: 10 October 2019, 16:00

Funding Available: Up to £9M (at 80% FEC) to support 4-6 research projects

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.

Key Dates:

Activity	**Date**
Call published	30 July 2019
Deadline for Full Proposals	10 October 2019, 16:00
Prioritisation panel	February 2020
Funding decision	March 2020

Additional information: Please note the three requirements in the Eligibility section below

Contacts: Miriam Dowle, 01793 444321, miriam.dowle@epsrc.ukri.org

EPSRC
Engineering and Physical Sciences Research Council

Security for all in an AI enabled society

Call type: Invitation for proposals

Closing date: 10 October 2019, 16:00

Related themes: Digital economy, ICT

Contents of this call document

Summary

The Digital Economy Theme, part of UKRI, would like to commit up to £9M (at 80% FEC) to support 4-6 research projects which address challenges that lie at the intersection between artificial intelligence (AI) and cyber security. This includes both security for AI and AI for security, aiming for better and more wide-spread adoption of trusted and secure AI systems across the UK's digital economy. We expect projects to take a fundamentally applied and interdisciplinary approach, across ICT, DE, social sciences and user communities.

Proposals will be sent to expert postal peer review before being assessed by a prioritisation panel composed of experts from academia, users and government representatives.

The National Cyber Security Centre (NCSC) and Defence Science and Technology Laboratory (Dstl) have been involved in determining the scope of this call. They do not have particular priorities within the scope of this call and are instead willing to work with all of the successful projects funded to help build a vibrant

community in this area within the UK. In order to facilitate this, applicants are expected to ring-fence some of their funding to support networking and community building activities. This should enable consolidation of research ideas, sharing of expertise and act as a focal point to effectively engage with other interested stakeholders including NCSC and Dstl.

Background

Systems which use AI in all its forms and at different levels of abstraction are becoming pervasive. However, they are not currently designed to be secure, trusted and accessible for everyone in society. There are also potentially huge benefits of exploiting AI to improve the security of our current and legacy systems.

Unless we can rely on the AI components to behave as expected, we cannot fully realise their benefits, regardless of progress and investment in AI. Robustness of AI systems need to be addressed early, prior to deployment. A sociotechnical context for improved understanding and trusted assurance of these dynamically evolving systems will create better adoption and acceptability.

While there is significant interest in the usage of artificial intelligence, this focuses on secure algorithmic and dataset design, which provide only one component for providing security for artificial intelligence. There is limited understanding of what is needed to keep intelligent tools secure throughout their lifecycle - from requirements scoping and data collection to implementation and maintenance through to their decommissioning. This whole lifecycle view needs to be fully explored to ensure potential weaknesses across the whole system are considered. Equally critically, across this lifecycle, human interactions – both regular users and adversaries – with AI tools and techniques need to be considered and how they may shape the behaviour of AI systems.

The intersection of AI and cyber-security is a very broad, topical area and we acknowledge that this call will not solve the entirety of the challenge. What we are aiming to do is create a portfolio of adventurous flagship projects which can demonstrate the viability of different research approaches and in so doing, build a critical mass foundation for research and innovation for the area in the UK.

Projects funded through this call must complement already existing activities currently underway in this complex landscape. EPSRC has already made significant investments in the area, including the Securing Digital Technology at the Periphery (SDTaP) investment through the Strategic Priorities Fund[1], a NetworkPlus[2] and two targeted research calls in Trust, Identity, Privacy and Security[3,4].

[1] https://epsrc.ukri.org/funding/calls/securingdigitaltechnologies/

[2] https://epsrc.ukri.org/funding/calls/networkplustips/

[3] https://epsrc.ukri.org/funding/calls/trustidentityprivacysecurity/

There are two strands for the intersection of artificial intelligence and cyber security - Security for Artificial Intelligence or Artificial Intelligence for Security. Applications to this call must address at least one of these two aspects.

Research Challenges

The research proposals should clearly address at least one aspect of the principle challenge areas.

- Security for Artificial Intelligence: Consideration of the design concepts, factors and evidence that are needed to provide artificially intelligent solutions that are demonstrably secure. This could include, but is not limited to, the following:
    - Securing Intelligent Systems across their whole lifecycle: Understanding how designers and developers of AI systems consider security issues and how particular design and implementation choices affect the security of AI is fundamentally important. Equally important is the need to consider the impact on security from the AI's ability to learn and adapt as well as the impact of regular users, maintainers and adversaries coming into contact with it throughout its lifecycle including decommissioning.
    - Understanding of attacks: including building an understanding of the types of potential attacks on these systems, behaviour of adversaries (whether human or AI), the practicalities of dealing with them, and developing techniques to defend against them.
    - Detection of Degradation of Behaviour: if the responses of a system adapt to its inputs over time how can we develop techniques to identify whether it is still behaving as it should? Can human or AI adversaries exploit the adaptive nature of the system to lead to such degradation? If the environment of a system is evolving over time, can we detect when the system is no longer able to behave as it should?
    - Data Supply Chains: The data sets that are used to train artificial intelligence may come from wide and varied sources. What metrics should we use to determine the quality of a training data set? How can we demonstrate that it is fit for the intended use? Alongside this, how can we build methods to secure the data gathering chain by default or detect when the data supply chain has been tampered with, and if not what are the inherent risks from not doing so?
    - Explainable AI: As part of the problem with many approaches currently utilised for AI, black box methods make it difficult to interrogate a system if something goes wrong. Could an AI system be able to explain its security properties and provide assurances about its security as it evolves? Could this be adaptable to different

[4] https://epsrc.ukri.org/funding/calls/tips2/

types of users and in different contexts? Could this introduce further security risks?

- Artificial Intelligence for Security: The use of artificial intelligence for providing the capability to deliver improved security. This could include, but is not limited to, the following:

    - Analysing and Utilising Outputs: The manner in which current network or security data is processed might not be the most efficient manner to provide usable security insights for end users. Identifying methods of understanding and working with uncertainty in the outputs of intelligent security tools could provide better security insights.

    - AI and Human Interaction: AI and humans have complementary abilities, how can these be harnessed to improve security? How can the human interactions be designed to minimise adding weakness to the security of an AI system? Conversely, how can human expertise augment the capabilities of an AI-based security system? And how does AI-driven security impact human responses in an emergency scenario?

    - Novel Approaches: While some aspects of using AI for security are well developed, what are the other potential applications that have not been considered, including its use in our current and legacy systems?

    - The AI Security Tool Lifecycle: With AI security tools being relatively new, thought needs to be put in to understanding the whole lifecycle of the product, including requirements, data gathering and processing, regulatory compliance, and safe and secure decommissioning.

The importance and impact of secure artificial intelligence is wider than just those of the security application. We seek proposals where the use case context means there is a viable need to secure the intelligent digital system. This could cover a variety of data intensive sectors, for example healthcare, transport, energy, retail, financial or environmental. All projects must be in partnership with a real-case user.

All applications must also structure their proposed research in order to deliver against all of the following requirements:

- Consideration of societal implications by design – individuals, communities and/or society.

- An “in the wild” application of the research within the lifetime of the project. This means the research should be applied in a real world context, using real data and working with real people.

- An appropriately multidisciplinary team to ensure the research challenge is tackled holistically, with both technical and social elements considered

thoroughly. Proposals submitted though this call must include investigator and research assistant time from more than one discipline. The novel aspects of the research must be more than half in EPSRC's remit.

- Deliver responsible research and innovation and constant monitoring of this.

We want to engender a sustained and collaborative approach so that these projects engage with the wider relevant sectors, stakeholders and disciplines both during and after the funding period. Sharing of best practise is therefore needed to enable the community to strengthen, and work to go beyond the initial funding. More details on how this should be requested in the proposal are below.

This scope aligns with the long-term ambitions within EPSRC's Strategic Delivery Plan to ensure that advanced digital technology is routinely used and reduce the risks and negative impacts it may have. It also addresses the Digital Economy's Trust, Identity, Privacy and Security (TIPS) priority and the ICT Theme's Safe and Secure ICT priority.

This call leads from recent (February and March 2019) discussions held with the EPSRC/NCSC Research Institute Directors and Academic Centres of Excellence in Cyber Security Research Directors and also broader contextual discussions at a Digital Economy Theme Strategic Workshop. Scoping discussions have been held with members of our strategic advisory boards, alongside our key user partners NCSC and Dstl.

For more information about EPSRC's portfolio and strategies, see our website: https://epsrc.ukri.org/research/ourportfolio/

Funding available

Up to £9M (at 80% FEC) is available to support 4-6 adventurous research projects. There is no restriction on the timeframe and it us up to the applicant to determine what is most appropriate for their project.

Proposed projects must have the following:

- An investigatory team drawn from more than one discipline
- At least one user partner who is committed to fully engaging with the research from the outset and will commit appropriate resources to enable this (cash or in-kind contributions)
- A plan to deliver an "in the wild" application of the research within the lifetime of the project. This means the research should be applied in a real world context, using real data and working with real people.
- A commitment to deliver responsible research and innovation, and a plan for how they will monitor this through the lifetime of the project

Funding can be requested for standard research activities and associated support but we do encourage applicants to take creative, adventurous approaches to research and request whatever they need to deliver that.

To build and maintain partnerships with potential users of the research, applicants can request resource to support secondments of researchers (either research assistants or investigators) in to user environments. Resource could also be requested to support secondments of people from user environments in to academic environments. Please note that user salaries cannot be supported by EPSRC funding and that a project partner listed in the Je-S form cannot directly receive funding from the grant.

Projects funded through this call should ring-fence 5% (of the total FEC proposal value) of their funding to support networking and community building activities across the successfully funded bids. The aim is for successful applicants to this call to work collectively and with other relevant stakeholders, including NCSC and Dstl, to strengthen the community. It is for applicants to determine the best use of these funds and deem what is most appropriate for the research programme. The costing and use of these networking funds must be clearly identified in the Pathways to Impact statement.

Full consideration of the implications of your work is important. Scientific research has the ability to not only produce understanding, knowledge and value, but also unintended impacts, questions, ethical dilemmas and, at times, unexpected transformations in social life. We recognise that we have a duty of care to promote approaches to “responsible innovation” which will initiate ongoing reflection about the potential ethical and societal implications of the research that we sponsor on behalf of the taxpayer and to encourage our research community to do likewise. Our aim is to build capacity within our research community to discuss and consider social and ethical questions. Therefore we expect applicants to work within the Framework for Responsible Innovation (AREA framework link below). Applicants could consider requesting support to fund activities run by ORBIT, which provides services to promote and support responsible research and innovation. More information about ORBIT can be found in the link below.

Public understanding and engagement is essential for work in this space and we encourage applicants to this call to request resources to enable this as part of the proposal. Examples include training in public engagement or communications, public engagement specialist staff expertise and support, materials/venue costs or travel expenses. Activities and related resources requested must have a strong link to the research proposed as we cannot support generic science outreach through this call.

Framework for Responsible Innovation (AREA):
https://epsrc.ukri.org/research/framework/

ORBIT: https://www.orbit-rri.org/

Media training: https://www.epsrc.ac.uk/innovation/publicengagement/

Equality, Diversity and Inclusion

The long term strength of the UK research base depends on harnessing all the available talent and the Research Councils have together developed the ambitious UK Research and Innovation Equality, Diversity and Inclusion Action Plan https://www.ukri.org/files/legacy/skills/action-plan-edi-2016/

In line with the UK Research and Innovation Diversity Principles, EPSRC expects that equality and diversity is embedded at all levels and in all aspects of research practice. We are committed to supporting the research community in the diverse ways a research career can be built with our investments. This includes career breaks, support for people with caring responsibilities, flexible working and alternative working patterns. With this in mind, we welcomes applications from academics who job share, have a part-time contract, need flexible working arrangements or those currently committed to other longer, large existing grants. Please see our Equality and Diversity webpages https://epsrc.ukri.org/funding/equalitydiversity/ for further information.

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/

Eligibility

To encourage full and committed engagement in the proposed work, applicants must ensure that:

- any single investigator appears on only one proposal, either as an principal investigator or co-investigator
- proposals include investigator and researcher time from more than one discipline
- proposals include at least one fully engaged potential user of the research

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 to apply to EPSRC 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 "Security for all in an AI enabled society" 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 10 October 2019.

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

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.
- Pathways to Impact: should be up to two pages and is primarily for detailing the activities which will help develop potential economic and societal impacts. Please detail how the proposed research project will be managed to engage beneficiaries and increase the likelihood of impacts. 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. Please note the requirement to ring-fence 5% of the funding for networking activities. 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.

- Work plan: should be up one page. It is not expected that this will be a Gantt chart for the whole time of the project, but should include a comprehensive plan for the start of the project and then refer to the management strategy to give appropriate milestones for when important decisions on the direction of the 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/

Assessment

Assessment process

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

Stage 1: Postal peer review

Proposals will be reviewed via standard postal peer review. 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

If the reviews are sufficiently supportive, the proposal will be assessed and ranked by a panel based on the reviewers' comments and the applicant

response, using the assessment criteria provided below. The panel will consist of cross-disciplinary researchers and will include relevant experts and users from across the area.

Assessment criteria

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

Fit to call (Primary):

- Addresses at least one of the principle challenge areas – Security for AI or AI for security
- A multi-disciplinary, application focused approach
- Consideration of societal implications by design – individuals, communities and/or society
- An “in the wild” application of the research within the lifetime of the project
- Responsible research and innovation and constant monitoring of this

Quality of research (Secondary Major):

- Novelty and timeliness
- Appropriateness of proposed methodology

National importance (Secondary):

- New activity that adds to recent investments in the area
- Responsible innovation has been considered and explored, and a plan for how it will be continually monitored has been provided

Pathways to impact (Secondary):

- Relevance and appropriateness of any beneficiaries or collaborators, evidence that the proposal has been co-created and developed in partnership to deliver maximum impact.
- Plans for dissemination and knowledge exchange.
- Appropriate resources have been requested to support 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, to ensure the research challenge is tackled holistically
- Demonstration of a culture of co-creation, with commitment from all partners to engage with each other throughout the research programme

Resources and management (Secondary):

- Effectiveness of planning and resource management strategy
- Appropriateness of resources requested

Feedback

Feedback will consist of reviewer's reports and, if they are sufficiently supportive, the ranking position at the prioritisation panel. The prioritisation panel may provide specific feedback if deemed necessary, but this will not be given 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/

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	30 July 2019
Deadline for Full Proposals	10 October 2019. 16:00
Prioritisation panel	February 2020
Funding decision	March 2020

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

Contacts

For general enquiries, including any questions about the call process or scope, please contact:

Miriam Dowle, Senior Portfolio Manager

Email: miriam.dowle@epsrc.ukri.org

Phone: 01793 444321

If you experience difficulties using Je-S or have questions regarding its use, the helpdesk can be contacted:

Email: JeSHelp@je-s.ukri.org

Phone: 01793 444164

Change log

Name	Date	Version	Change
Miriam Dowle	15 July 2019	1	N/A
Miriam Dowle	30 July 2019	1.1	Corrected deadline and error in bullet point formatting on page 9

Appendices

Je-S attachments Check List

Standard:

Attachment Type	Maximum Page length	Mandatory / Optional	Extra Guidance
Case for Support	Eight pages	Mandatory	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	Mandatory	
Workplan	One page	Mandatory	
Justification for Resources	Two pages	Mandatory	
CVs	Two pages each	As required by EPSRC	For named post doctoral researchers, visiting researchers and researcher co-investigators only.
Project Partner Letters of Support	No page limits	As required by EPSRC	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	As required by EPSRC	In exceptional circumstances a maximum of three letters can be submitted.
Proposal Cover Letter	No page limit	Optional	The cover letter can be used to highlight any important information to EPSRC. 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.