UK Research and Innovation

Quick Reference

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

Establishing a Research Centre for Securing Digital Technologies at the Periphery

Call type: Invitation for a single proposal

Closing date: 16:00, 4 December 2018

Funding Available: Up to £13 million is available to create a single national Research Centre.

How to apply: This will be via a single stage submission

Assessment Process: The full proposal will be considered by an expert interview panel

Key Dates:

Activity	Date
Deadline for Full Proposals	4 December 2018
Interview Panel	17 or 18 December 2018
Grant start date	1 January 2019
Grant end date	31 March 2023

Additional information:

This strategic investment is building on the existing PETRAS activity and therefore eligibility to lead the application for this call is restricted to the PETRAS leadership team.

Contacts:

- John Baird, Head of Digital Economy Theme (John.baird@epsrc.ukri.org)
- Miriam Dowle, Senior Portfolio Manager, Digital Economy Theme (Miriam.dowle@epsrc.ukri.org)

UK Research and Innovation

Establishing a Research Centre for Securing Digital Technologies at the Periphery

Call type: Invitation for a single proposal

Closing date: 16:00, 4 December 2018

Related themes: Digital economy, ICT

Summary

EPSRC, on behalf of UKRI, is seeking to make a step-change in the broad research areas of cybersecurity, designing in trust, privacy, security and resilience associated with the Internet of Things (IoT) through this call. This will establish a Research Centre focusing on Security of Digital Technologies at the Periphery (SDTaP). This will be a centre of excellence to provide a national capability to enable the UK to become a world-leader in IoT security and associated systems security through new knowledge and deep expertise creation. The research focus will be on the challenges associated with privacy, security and trust in the IoT, including the various interactions, policy and governance, beliefs and behaviours between people and emerging IoT systems that include 'Edge Computing' AI and Machine Learning.

It will build on an existing successful UK Research and Innovation activity as part of the broad IoT portfolio, which includes the interdisciplinary Privacy, Ethics, Trust, Reliability, Acceptability and Security (PETRAS) IoT cybersecurity Research Hub. It will combine experimental and applied research in an emerging and important field – where connected (and increasingly) intelligent devices form the "periphery" of the Internet.

Originally PETRAS was set up with a five year time frame in mind, however, due to funding restraints at the time it has only been able to run for three. UK Research and Innovation is now investing in this second, expanded phase of PETRAS. There is up to £13 million available to invest until 31 March 2023, to create a National Centre. The intention of this call is to open the development of the proposal to excellent research expertise across the UK to collaborate and work together in a consortium, not to compete with each other. The members of the centre will work in partnership in an integrated manner, across the relevant disciplines, addressing the research challenges in a coordinated way to form the research centre programme. They will harness and build on existing multi/interdisciplinary knowledge and skills, and also address intellectually inspiring and user-led challenges. Partners will need to demonstrate how they can contribute to meeting the objectives of the research centre. It is expected that most new academic partners will become engaged mainly through funding

calls which will be run during the Centre's lifetime. A key objective is to maintain the critical mass of staff and expertise of PETRAS, without any gap in capability, and, at the same time, expand the remit to cover new aspects. This includes attracting business partners, with associated funding, alongside the new academic partners.

Please note, we will only accept a single bid to create a Centre of National Excellence and we expect this to be coordinated by the current PETRAS leadership team. This should include relevant researchers and Research Organisations to create a world-leading Centre.

The proposal will be submitted by 4 December 2018. Peer review will be by an interview panel with members drawn widely from recognised experts across the disciplines. It will include appropriate representation from relevant government stakeholders and UKRI Advisory Bodies. The Research Centre should commence in January 2019. It will segue into relevant activities supported by the existing PETRAS Research Hub allowing the transfer of appropriate people from one to the other.

Ultimately, as well as the economic benefits of leading a major new technology application, UK progress on the IoT and associated systems, will deliver life-changing improvements for citizens and cost and efficiency savings, particularly if designed in a user-focussed and people-centric way. The creation of real usable knowledge and impact (be it economic, societal or cultural) will help to cement the UK's position as a world leader in this area.

Background and scope

Our society, homes, workplaces and infrastructure are increasingly connected to the Internet by sensors and devices, creating an "Internet of Things" (IoT) world. The integration of information from IoT devices is already transforming our everyday lives.

There are many forecasts for the size of the global IoT market; a Forbes report[1] gives a roundup of IoT growth forecasts as of December 2017. All indicate it will be very large and growing fast. According to Growth Enabler[2] , the global IoT market share will be dominated by three sub-sectors; Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%). Followed by Smart Homes (14%), Connected Cars (7%), Smart Utilities (4%) and Wearables (3%).

This IoT-enabled world offers huge potential, not only measuring our health data, travel habits and energy consumption, but also aiding understanding and automating control in our critical national infrastructure, such as power stations and transport networks. These new structures allow more interactions with people, often with unprecedented access to information and decision making based on that data, which is often personal.

The more devices connected, the more links and dependencies between systems are created. This potentially presents significant risks, with cybersecurity emerging as the predominant threat to inter-dependent systems; there is a need

[1] https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#a4165981480e

[2] https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

to have assurance that systems will behave appropriately, even in unforeseen circumstances, and be resilient.

Humans are one of the most vulnerable parts in IoT augmented systems, but also have a fundamental role in their safety, security and resilience. Behavioural aspects of end users, of system operators and of the threat actors must be considered together with system behaviour and ways in which humans and systems adapt to each other.

Learning from the broad-reaching mid-term findings of PETRAS, we are able to see short and longer-term focus areas requiring more intensive socio-technical research coverage. The Growth Enabler report highlights these findings - Smart Cities, Industrial IoT, Connected Health, Smart Homes and Connected Cars – are rapidly emerging application areas for at-scale deployment of IoT and in due course, "AI at the Edge of the Internet".

This call builds on an existing successful UK Research and Innovation asset: the interdisciplinary Privacy, Ethics, Trust, Reliability, Acceptability and Security (PETRAS) IoT cybersecurity Research Hub. This was originally funded as an activity within IoTUK (https://iotuk.org.uk/) from the ComPaTrIoTS call (Commitment to Privacy and Trust in Internet of Things Security (https://epsrc.ukri.org/files/funding/calls/2015/iotresearchhub/)). As outlined in the ComPaTrIoTS call, the raison d'etre for having a security focus for IoT activities remains. The December 2014, Blackett Review "*The Internet of Things: making the most of the Second Digital Revolution*"[3] explored how the UK can make best use of the IoT. Although there are many significant research challenges in the IoT space, a fundamental and underpinning issue was the need for research to ensure that appropriate security, trust, ethics and privacy are designed and implemented from the beginning.

The funding for the first phase of PETRAS runs out in February 2019, well before its full potential can be realised. When PETRAS was originally set up it was anticipated that it would run over a longer time frame. Funding restraints at the time allowed for three years of activities, but UK Research and Innovation is now investing up to £13M in this second, expanded phase of PETRAS, until 31 March 2023. Since being established in 2015, major research progress has been made through PETRAS, which involves eleven universities and over 110 user partners. PETRAS has developed an internationally recognised brand and reputation as a high profile UK asset[3]. It has excellent industry linkages and an impressive track record of impacts on policy and research helping to set the agenda in many instances[4]. PETRAS has already attracted cash and in-kind support of over £14 million from its user partners. It is assumed that this leverage and influence will be maintained into the next phase. In a recent independent review of IoTUK, PETRAS is cited as having "output delivery…far higher than expected"[5]. One objective is to build on lessons learnt over the last three years during the IoTUK programme.

[3] The PETRAS Standards, Governance & Policy stream provided strong and acknowledged inputs to the DCMS 'Secure by Design' report, recently published https://www.gov.uk/government/publications/secure-by-design.

[4] Two peer reviewed joint reports from PETRAS and the Royal Academy of Engineering Cyber safety and resilience: strengthening the digital systems that support the modern economy and "Internet of Things: realising the potential of a trusted smart world" https://www.raeng.org.uk/news/news-releases/2018/march/improving-cybersecurity-requires-major-coordinated).

[5] https://www.gov.uk/government/publications/interim-evaluation-of-the-internet-of-things-uk-research-and-innovation-programme-2015-2018

The aim of this call is to establish the next phase of PETRAS, as a challenge-led, national capability. This interdisciplinary Centre will tackle challenges through a combination of experimental and applied cybersecurity research, engaging with the public, bridging disciplines and bringing together research communities to jointly address challenges. Drawing on existing wide interdisciplinary expertise spanning technical and behavioural sciences, law and ethics, it will combine experimental and applied research in an emerging and important field – where connected (and increasingly) intelligent devices form the "periphery" of the Internet.

Funding available

The funding available is up to £13 million until 31 March 2023, and is on a scale needed to create one national centre of excellence to maintain and enhance the UK's capacity and capability in this field.

The Centre will be an internationally recognised beacon for IoT research leadership, led by a small number of leading UK universities working together across the relevant disciplines, addressing inter-related and interdisciplinary research and situated on existing University campuses.

The funding is at 80% of the Full Economic Costs typical of Research Council grants. This means the remaining 20% will be funded by the host Universities.

It is anticipated that a significant proportion of this funding (at least 30%) will be used to fund projects through calls that would enable new partners to join the research programme. This will facilitate best-with-best collaboration in the UK or internationally, both with academic and user partners.

There will be interaction with a number of Demonstrators that Innovate UK will establish in this area. A joint governance board will ensure alignment of objectives and outcomes.

Activities supported in the Research Centre

As is already undertaken by PETRAS, the expectation is that the research supported will be more applied than blue sky. However, this does not preclude the inclusion of more fundamental challenges necessary to make progress in this area. Overall, the research should be grounded in 'real world' applications and have close involvement with potential users.

The Research Centre must be interdisciplinary and have strong and significant partnerships with a range of commercial and public users, including the third sector.

Topics and challenges of interest include:

Building Public Value at the Edge: Connected IoT devices provide many avenues for public good, including increased understanding of the world to support policy interventions; new innovative goods and services; and information to help safeguard individuals. Many of these insights come from the combination of IoT with AI but new challenges emerge in processing the data at the edge in a way that preserves privacy, security and trust yet yields the same benefits. How can we secure, decentralised computing or 'AI' applications in realistic IoT deployments? Do users trust these systems and approaches, and in which contexts? How can we defend against new threats such as poisoning of sensor

data or exploiting the vulnerabilities of AI? How do privacy and security preserving approaches affect other tasks such as anomaly detection, or repurposing data for entirely novel applications? How can important information such as around measurement quality or data provenance, be obtained and combined with data from sensors themselves? Finally, how do and might approaches to building public value using these new technologies coexist with existing and emerging legal frameworks?

Securing the Connected Edge: An IoT-augmented physical reality is open to adversarial behaviours that are yet unchartered and poorly understood, and that span the sociotechnical dimensions. The impact of compromise needs to be evaluated in terms of its resulting consequences on end system provision and its safety implications. The resilience of systems in their physical, digital and social dimensions needs to be ensured. How can systems adapt to continue to operate safely and securely when they have been compromised? How do they recover and become more robust? How can AI help defend, adapt and recover systems in response to adverse events? How can we assure systems that continuously adapt and employ AI techniques and how can we understand and mitigate the vulnerabilities of such techniques? How do users and autonomous systems interact with each other to ensure system resilience? How do we maintain security and resilience with legacy devices? What are the social and technical routines needed to stress-test systems for complex attacks?

Useful and Useable Decentralised Systems: There is a gap between autonomy on paper that decentralised systems promise to edge-users, and the control that edge users feel capable and able to exert, particularly given the number of decisions they are expected to make in this data-saturated world. Research in psychology and human-computer interaction is needed to point to how decentralised systems can be useful and useable in practice, rather than only in theory. This in turn is likely to trigger new questions for security researchers, for example in areas such as identification and interoperability. What can and should the users' roles in securing systems be, and how do technical aspects of IoT security interact with these human factors? Further to this, how do users work together to achieve their goals in a decentralised system? What methods of collaboration, both online and offline, can help individuals achieve their varied goals in their home environments, workplaces, and urban surroundings?

Law and Economics at the Edge: Business models for IoT systems, particularly those undertaking decentralised analytics, are still emerging. What are the main considerations in areas such as measurement, transactions and demand management in these systems? Which new marketplaces and financing mechanisms might they in turn open up the opportunities to create? Emerging business models and IoT systems with analytic components are also likely to touch upon a wide array of legal and governance provisions, such as data protection law, competition law, liability and platform regulation. How do these regimes cope with these systems, and what are the major tensions they highlight or changes they would require to succeed? What does, should, and could standardisation of these systems look like in national and international policy fora?

Activities that maximise impact and enable cross-partner working will be expected. Some suggestions for the form these impact activities could take include:

- Fundamental, applied or translational research that has clearly identified and engaged stakeholders (for challenge, evaluation, and possible adoption), particularly that arising from the associated SDTaP demonstrators and previous IoT UK activity;

- Knowledge exchange and early stage 'proof-of-concept' activities that are essential to securing credible and engaging impact and commercial opportunities of all kinds. Where appropriate, it could help researchers to bridge the funding gap between traditional research grants and commercial funding and attempt to move the outcomes and outputs of this work to the next stage of impact.

- 'In the Wild' deployment and evaluation, to realise more effectively the impact of the research. This could either cover the testing of new technologies and methods with potential beneficiaries or in the user(s) domain or looking at new ways of using existing technologies/methods. 'In the Wild' is intended as a research methodology, where some of the design is through usage; this is particularly important in the IoT.

Additional funding and leveraging requirements for the Research Centre

There must be demonstrable support for the research from user partners (public, private or third sector) from the start of the project. Adequate leveraging and funding arrangements must have been agreed. Ideally co-funding and leveraging will be in place up front but user partners can have flexibility to back-load their commitment and support over the life of the Research Centre. A demonstration of 100% matched funding (either cash or in kind) is expected to be in place by the end of the project. The host organisation(s) will also be expected to demonstrate substantial support for the Hub through cash and/or in-kind contributions (please note 20% FEC contribution to any funded grant will count towards the consideration of matched funding).

Research Centre Requirements

In summary, the Research Centre for Securing Digital Technologies at the Periphery must demonstrate:

1. **Critical mass, breadth and interdisciplinary nature to create a National Centre of Excellence.** It is important that the Research Centre consists of university partners with the appropriate disciplinary coverage across the diverse aspects of the research. This will create internationally recognised leadership for the UK.

2. **Strong interaction with the demonstrators**, supported by Innovate UK, to address intellectually inspiring and user-led challenges arising from the demonstrators and other associated activities.

3. **How impact will be maximised through the centre's specific project plans**, for example by addressing clearly defined research challenge(s), demonstrating how they have been co-created with the end-user(s), through undertaking research 'in the wild' and appropriate knowledge exchange and early stage 'proof of concept' activities.

4. **Leveraging and additional funding**. Substantial support from university and user partners must be demonstrable, as discussed above, as well as collaboration and engagement with innovative businesses including SMEs.

5. **Strong people support**. Demonstrate that mechanisms are in place within the centre to grow and develop the pool of trained interdisciplinary researchers, including transitioning early career researchers into academic and industry leadership posts, ensuring that user-led interdisciplinary research and culture is maintained beyond the life of the centre.

6. **Partnership resource fund** of up to 10% of funding in a flexible manner to help engagement with industry, particularly SMEs and responding to user-inspired challenges.

Management of the Research Centre and other activities within the Securing Digital Technologies at the Periphery Programme of work

The overall programme of work covered by the Securing Digital Technologies at the Periphery activity covers two main aspects - the Research Centre and a number of Demonstrators.

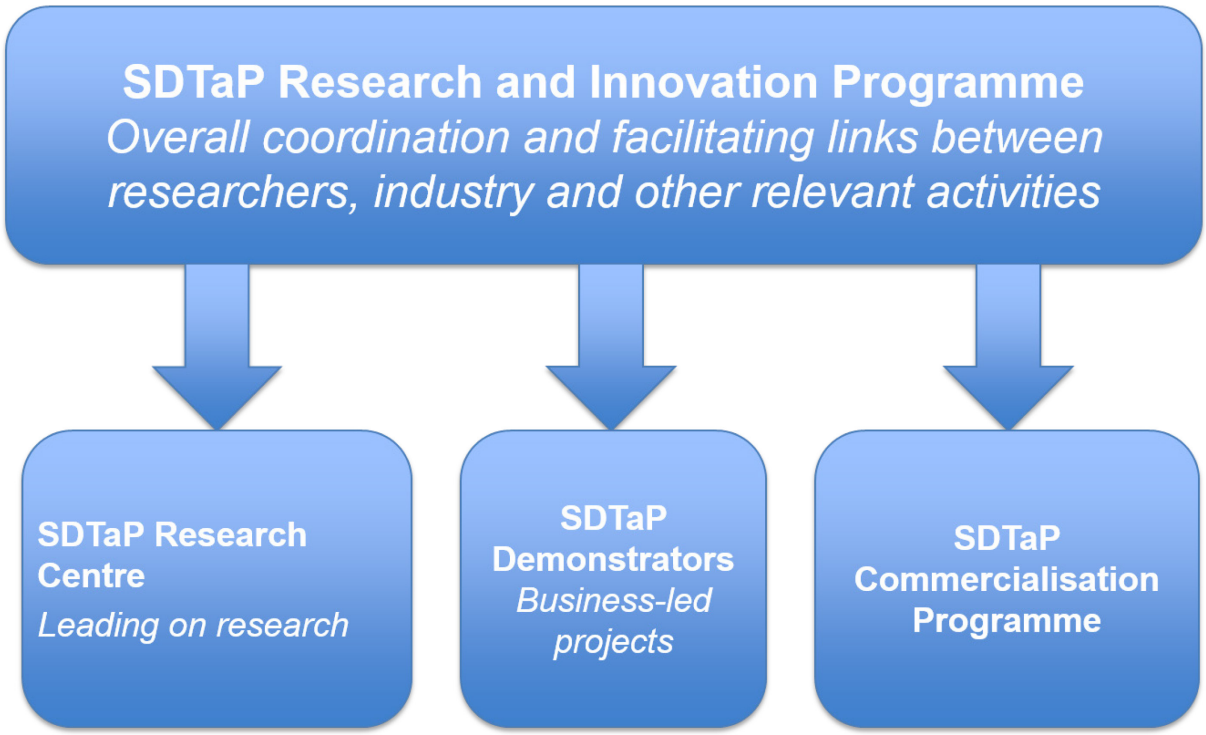
An independent governance and advisory board should be formed to allow overall coordination and facilitate links between researchers, industry and other relevant activities. It should comprise representatives from InnovateUK and EPSRC (and other Research Councils in whose remit this lies, such as ESRC and AHRC) and the innovation and research community including users. This will cover operational matters to account for hitting key milestones and deliverables for the overall SDTaP activity (see diagram below). The SDTaP Centre will be a complex and dynamic organisation, and its governance and management must accommodate this. It should also align with existing monitoring frameworks used by EPSRC (for the Research Centre) and Innovate UK (for the demonstrators)

Under an independent Chair from a key private sector partner organisation, the constitution of the Steering Board comprises three groups:

1. Key strategic users from public and private sector

2. Funding body stakeholders

3. SDTaP PI, Co-Investigators, and other key members



How to participate in the National Centre proposal

The aim of this exercise is to create a National Centre of Excellence, building on the work of PETRAS, but with the second phase including relevant excellent researchers from across the UK. It is expected that new academic partners will become involved mainly through funding calls that the centre will run during its lifetime. These calls will be open to the whole community and the centre will be mandated to issue an early call for new academic collaborators to join. Partners will need to demonstrate how they can contribute to meeting the objectives and remit of the research centre.

In addition, researchers who believe they have the excellence, ambition, critical mass, multi-disciplinary expertise, strategic alignment and appropriate user partner engagement and collaboration to meet the challenges and wish to join the consortium as part of the proposal to be submitted by 4 December 2018, need to make contact with EPSRC via digitaleconomy@epsrc.ukri.org. EPSRC will put you in touch with the appropriate contact in PETRAS. In view of constraint in the timetable, any discussions would need to take place by mid-November 2018. It is not anticipated that any more than a small number of new University partners would wish to be involved at this stage.

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 UKRI Equality, Diversity and Inclusion Action Plan (https://www.ukri.org/files/legacy/skills/action-plan-edi-2016/).

In line with the UKRI 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 at 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

We will only accept a single bid to create a Centre of National Excellence and we expect this to be coordinated by the current PETRAS leadership team. Please see section entitled "How to participate in the National Centre proposal" for more details. This should be submitted as a single JeS submission.

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 "Securing Digital Technologies at the Peripheral (SDTaP) Research Hub"

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 4 December 2018.

We will only accept a single proposal on Je-S, led by one institution. Other academic partners involved in the bid should be listed as co-investigators.

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/howtoapply/) which should be consulted when preparing all proposals.

Guidance on writing an application

Please see the attachment checklist at the end of this document for a list of required attachments.

In addition to the standard requirements, technical annexes and a management plan should be included within the case for support. Page limits for these can be found at the end of this document.

Letters of support from all research organisations involved in the consortium should be included in the application, detailing leveraged funding and collaborators involved. Please combine all letters of support from consortium research organisations in to one PDF file and submit as a single attachment.

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://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

Peer review based on the assessment criteria will be by an interview panel with members drawn widely from recognised experts across the relevant disciplines. It will include appropriate representation from relevant government stakeholders and UKRI Advisory Bodies.

A break will be incorporated in to the interview schedule, in order for the panellists to confer and decide on any additional points for clarification.

Written feedback will be given to applicants following the interview.

Assessment criteria

Relevance to the objectives of the call, in particular; (Primary)

- The Centre can demonstrate the critical mass and coherence needed to address the interdisciplinary research requirements
- Appropriateness of activities designed to maximise impact and user engagement (for example demonstration of research challenge(s) being co-created by end-user(s)) and has specific project plans in place to deliver this;
- Degree of partnership support, leverage and funding;
- Appropriate people support mechanisms are in place to grow and develop the pool of interdisciplinary trained researchers, ensuring the sustainability of user-led interdisciplinary research and culture beyond the life of the centre;

Quality of research, including: (Primary)

- Novelty, relationship to the context, and timeliness;
- The ambition, adventure and transformative aspects identified;
- Appropriateness of proposed methodology;
- Intersection of intellectual challenges, including with those identified by the Centre partners;
- Synergy and added value of proposed research strands.

National importance including: (Secondary Major)

- How the proposal contributes to, or helps maintain the health of other disciplines; contributes to addressing key UK societal challenges and/or contributes to future UK economic success and development of emerging industry(s);
- How the proposal meets national needs by establishing/maintaining a unique world-leading activity;
- How the proposal complements other UK research already funded in the area, including any relationship to the EPSRC portfolio.

Potential research impact, including: (Secondary Major)

- Relevance and appropriateness of any beneficiaries or collaborators (e.g. upstream engagement/co-design);
    - Suitability of the approach to engaging with other researchers (and new partners) to create a National centre of Excellence in IoT Cybersecurity
- Adequate plans for dissemination and knowledge exchange;
- Appropriateness of plans for promoting cross-disciplinary culture.

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

- Strength of the proposed team's track record and the leadership quality of the Principal Investigator;
- Balance of skills of the project team and integration of different methodologies and approaches.

Resources and management, including: (Secondary Major)

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

Additional grant conditions (AGCs)

Grants will be subject to the standard grant conditions in addition to specific conditions for this call. These will concern a fixed start date and additional reporting, and there may be further conditions added after interview.

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***
Deadline	16:00, 4 December 2018
Interview	Week beginning 17 December 2018
Grant start date	1 January 2019
Grant end date	31 March 2023

*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

- John Baird, Head of Digital Economy Theme (John.baird@epsrc.ukri.org)
- Miriam Dowle, Senior Portfolio Manager, Digital Economy Theme (Miriam.dowle@epsrc.ukri.org)

Change log

Name	**Date**	**Version**	**Change**
Miriam Dowle	5/11/2018	1	N/A

Appendices

Je-S attachments Check List

Standard:

Attachment Type	Maximum Page length	Mandatory/Optional	Extra Guidance
Case for Support	8 pages + Management Plan + Technical Annexes	Mandatory	Comprising up to two A4 sides for a track record, and six A4 sides describing proposed research and its context. Technical support annexes may be included to provide additional information on the research proposed. These can be up to two pages for each major research challenge identified. A Management Plan of 2 pages maximum should also be included
Pathways to Impact	2 pages	Mandatory	
Workplan	1 page	Mandatory	
Justification for Resources	2 pages	Mandatory	
CVs	2 pages each	Optional	For PDRAs, visiting researchers, and researcher co-investigators only.
Project Partner Letters of Support	No page limits	Mandatory for all project partners	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	Optional	A maximum of three letters from non-project partners can be submitted. Please combine all letters of support from consortium research organisations in to one PDF file and submit as a single attachment.
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.
Other Attachment	No page limit	Optional	

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.