Quick Reference

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

Scheme to Recognise Academic Centres of Excellence in Cyber Security Research (ACEs-CSR)

Call type: Call for participants

Closing date: 16:00 on 26 April 2019

Funding Available: Universities recognised as an ACE-CSR will each receive a grant of up to £60k (£48k at 80% FEC) from EPSRC to be used to support activities associated with recognition.

How to apply: We are inviting applications, through an online form on the EPSRC website, to be recognised as an ACE-CSR.

Assessment Process: Applications will be assessed by an independent expert panel, comprising members from government, industry and academia. All applicants meeting the criteria will be recognised as an ACE-CSR.

ACE-CSR recognition is given at an institutional level and EPSRC will only accept one application from any institution. Multiple applications from the same institution will not be assessed and will all be rejected.

Key Dates:

Activity	**Date**
Call opens	30 January 2019
Deadline for applications	16:00, 26 April 2019
Assessment panel	June 2019
Decision communicated	Week beginning 24 June 2019
Recognition start date	01 July 2019, for three years

Contacts:

- Miriam Dowle, EPSRC Senior Portfolio Manager (Miriam.dowle@epsrc.ukri.org)

Scheme to Recognise Academic Centres of Excellence in Cyber Security Research

Call type: Call for participants

Closing date: 16:00 on 26 April 2019

Related themes: Digital Economy, ICT

Summary

UK Government and its delivery partners are continuing their joint work to enhance the UK's academic capability in all fields of cyber security. As part of that work, EPSRC and the National Cyber Security Centre (NCSC) are leading on a scheme to recognise UK Academic Centres of Excellence in Cyber Security Research (ACEs-CSR).

This is the sixth call for UK Higher Education Institutions to submit applications to be considered for ACE-CSR recognition.

Recognition as an ACE-CSR is at the HEI/university level. We are looking for institutions whose cyber security research is of internationally notable scale, quality and impact.

This call is separated into two components which must both be completed:

- a proposal for recognition as an ACE-CSR, submitted through an online form on the EPSRC website
- a proposal for a grant from EPSRC to be used to support activities associated with recognition, submitted through Je-S

Further details are available in the "Submitting an Application" section of this document.

Background

Cyber security

The UK Government aims to ensure that the UK, its people and its businesses are secure, confident, agile and prosperous in cyberspace, and equipped with the knowledge and capabilities needed to maximise the opportunities and balance the risks of the digital era. Cyber attacks continue to create a Tier 1 risk as judged in the National Security Risk Assessment of 2015 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf] while the cyber-related aspects of many other risks highlighted in that document continue to be of great concern.

Research and innovation carried out by the UK's thriving academic and business sectors underpins our world-leading cyber security capability. The ACE-CSR scheme continues to be a key part of Government's approach to maintaining and enhancing the UK's reputation as a global leader in cyber security research.

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

Aim and benefits of the scheme

The overall aim of the scheme is to identify and give due recognition to those UK Higher Education Institutions carrying out cyber security research of sufficiently high quality, scale and impact across a reasonable range of cyber security knowledge domains as described in section titled "Knowledge domains relevant to this scheme". This will enable a better understanding of the UK's academic cyber capability, identify areas where there are research opportunities or technical gaps and so create a sound basis for future development of investment priorities.

Recognition is at the HEI/university/Research Organisation. It is based on the combined capabilities of the whole organisation rather than being applied to a particular faculty, school, department or research group. Once recognised, we expect HEIs/universities which are ACEs-CSR to take an integrated and inclusive overview of their cyber security research and training capabilities and to continue to develop them in that light.

An institution whose submission is successful in this Call will be able to hold the title of 'Academic Centre of Excellence in Cyber Security Research' for a period of three years, subject to complying with appropriate terms and conditions of membership of the scheme. They will also be supported by an EPSRC research grant (see section entitled "Funding Available").

The scheme makes collaboration and knowledge sharing between the best of the UK academic sector, business and government easier. It encourages exploitation of current leading-edge research and the identification of the future work needed to ensure the UK is well prepared to meet current and future cyber security challenges and threats.

ACE-CSR recognition raises the profile of a recognised institution's cyber security research efforts among students, peers, government and business. It is a visible indicator of quality, and of an institution's long-term commitment to the area. The scheme criteria provide a useful benchmark for the general academic community, encouraging cyber security activity to grow, and improving the quality and breadth of cyber security research across the UK.

ACEs-CSR work closely with government stakeholders. To help facilitate effective interactions, all ACEs-CSR will have a Liaison Officer from the NCSC or another government stakeholder organisation assigned to them. There will be an annual conference to which representatives from ACEs-CSR, government and business will be invited. Recognition as an ACE-CSR allows access to studentship funding through the NCSC's Sponsored Doctoral Studentships Programme.

Research needs within the scheme

The cyber threat is the source of many broad challenges for academic research. The layered, composite nature of today's cyber systems means that cyber

research challenges tend to be rapidly evolving and that they add to or modify, rather than replace, existing issues. They require new approaches, insights and techniques (for example those leveraging the power of data science) which can build on and work alongside continuing activity in more established areas such as cryptography, malware analysis and intrusion detection.

Areas that may not traditionally have been considered to be enablers of better cyber security, such as behavioural science and economics, continue to assume an increasingly important role in the field. We expect that recognised ACEs-CSR will reflect this trend.

Funding available

Universities recognised as an ACE-CSR through this call will each receive a grant of up to £60k (£48k at 80% FEC) from EPSRC to be used to support activities associated with recognition. Full details of the costs allowed and the process for applying are detailed in Annex A of this document.

All applicants meeting the criteria will be recognised as an ACE-CSR.

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 is not available through this call.

Eligibility

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/

ACE-CSR recognition is given at an institutional level and EPSRC will only accept one application from any institution. Multiple applications from the same institution will not be assessed and will all be rejected.

How to apply

Submitting an application

Applications for recognition as an ACE-CSR should be submitted via the online form on the call page on the EPSRC website (https://epsrc.ukri.org/funding/calls/acecsr2019/) by 16:00 on 26 April 2019. Full details on the contents of an application can be found in the Required Structure of application below.

You will need to submit a separate application through Je-S for the EPSRC support grant. Further details of this process are detailed in Appendix A of this document.

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

An application consists of six separate documents, each of which should be submitted through the online form on the call page on the EPSRC website (https://epsrc.ukri.org/funding/calls/acecsr2019/). Please note that there is an upper limit of 50MB per document. The documents should be submitted as:

1. 'Institution's Letter of Support for Application' (up to **one** side of A4)
2. 'Case for Recognition', which should include details of the research environment, vision and strategy (up to **three** sides of A4 in total) plus a knowledge domains matrix (described below)
3. 'Track Record and Esteem Indicators of Members of Staff' (no more than **two** sides of A4 per CV, combined into a single document)
4. 'Notable Publications' (no more than **one** side of A4 per member of staff, combined into a single document which contains accessible web links to publications)
5. 'Doctoral Level Students Programme' (page limit not specified though there is a general requirement for brevity)
6. 'External Research Funding and Impact of Projects' (up to **three** sides of A4 in total)

Documents should be in PDF format with the font size no smaller than 10pt. Additional documents and information will not be assessed. Your application should be based on evidence (e.g., permanent members of staff) that is correct on the 'Census Date' of **01 December 2018**.

Required structure of application

This section provides details of the information that you will need to provide with your application, and also the criteria against which it will be assessed. Please do

not include links to any additional documents or external evidence other than the publications included in the 'Notable publications' section

1. Institution's Letter of Support for Application

Please provide a signed letter from the Vice Chancellor (or equivalent) confirming that the institution is applying to be considered as part of the Scheme. ACE-CSR recognition will be recognised at an institutional level and we will only accept one application from any institution. Multiple applications from the same institution will not be assessed and will be rejected.

2. Case for recognition

Applications should refer to all elements of cyber research capability across the whole organisation. Please ensure that you include sufficient, succinct but detailed information to adequately describe the following:

a) The strategy and vision of the organisation in relation to developing its cyber security capability over the next three years. This might include the focus of its research or a developing research strategy; management (including the names of the proposed Principal Investigator and their core team), leverage and utilisation of its cyber security capability; and plans for sustainability and growth.

b) The names and structure of the department(s) /group(s) /school(s) where your organisation's cyber security capability may be found, together with the names, seniority and roles of permanent members of staff. (For these purposes, permanent members of staff are those eligible to be Principal Investigators on a Research Council grant [http://epsrc.ukri.org/funding/howtoapply/basics/eligibility].) Post-doctoral researchers at Senior Research Associate level (or equivalent) may also be included in the submission. However, to be suitable for inclusion, non-permanent academic staff must be undertaking independent, relevant research of a very high standard in which they are demonstrably providing thought leadership. They must also be funded on contracts that have at least three years to run on the Census Date of 01 December 2018.

c) Your organisation's cyber capability as it currently stands, including areas of cyber security research currently being undertaken, the organisation's development of these over the past five years or so, and any relevant facilities, laboratories, etc.

d) Recent strategic investments in relevant areas made by the organisation, government, business, etc.

e) A synopsis of the research currently undertaken by the members of staff named in 2b above in the form of a research matrix similar to the one below.

Criteria to be applied

Knowledge domain		Staff member A	Staff member B	…
Cryptography, key management and security protocols	• Cryptographic Primitives, including all aspects of cryptographic algorithm and primitives design and manufacture • high-function cryptography (identifier-based, attribute-based, homomorphic) …	full	partial	
Socio-technical Security …	• Communicating Risk • Cybercrime	…	full full …	

To be recognised as an ACE-CSR your organisation must have an established, cohesive, integrated and relevant cyber security research programme. You must be able to present a clear research focus, strategy and vision. There should be a minimum of five permanent, named members of staff who demonstrate a track record of, and potential for future, working together in areas which are demonstrably relevant to recognisable significant challenges in cyber security. While experience from previous rounds of the call suggests that, beyond this minimum threshold, the number of staff associated with the case for recognition is less important than the combined relevance and quality of their work. The technical areas to which each member of research staff contributes (whether fully or partially) should be clear, and claims of relevance to security must be supported by evidence rather than merely asserted.

If required, applicants may also provide succinct information explaining how many 'others' are involved in the Centre or in research grants (for example business support or development staff, post-doctoral researchers or programmers) and how intrinsic they are to the functioning of the Centre or individual projects. When providing such information, applicants should do so in order to demonstrate that there is a well-funded research environment that is well-equipped and supported across the whole organisation.

Any and all claims made in the ACE-CSR application may be investigated by the assessors. Therefore, applicants should take care not to overstate the relevance or level of activity being undertaken and should ensure, as far as possible, that claims made are supported by information available from other sources, for example: the University's web pages, on-line research paper repositories,

EPSRC's Grants on the Web. Claims which cannot be substantiated are unlikely to persuade the panel, and may in fact undermine the broader case you make.

3. Track Record and Esteem Indicators of Members of Staff

Please provide a CV for each of the members of staff named in section 2b of the application. The CV should clearly describe academic and other relevant experience, current role, the contribution made to cyber security research within your organisation, and a list of key relevant publications. The CV should also contain any relevant esteem indicators such as: journal editorship, programme committee membership, invited talks, membership of working groups or advisory groups, and Fellowship of professional bodies or learned societies.

We recognise that some staff members may have diverse career pathways. This includes career breaks, support for people with caring responsibilities, flexible working and alternative working patterns. With this in mind, we welcome the inclusion of staff members who job share, have a part-time contract or need flexible working arrangements.

Criteria to be applied

The CVs should clearly demonstrate that named staff have a proven track record and depth of experience in cyber security research and that this is recognised by the research community at large. Each CV should be consistent with the research matrix shown in the 'Case for recognition'. Our experience in earlier calls is that off-the-shelf CVs are not likely to be suitable and that some customisation and standardisation in order to draw out the areas relevant to this call will be beneficial. Similarly, the number of items included in the CV is less relevant to the assessment process than their relevance and quality.

It is strongly recommended that applicants avoid the temptation to over-claim and ensure that statements of expertise by individual academics are clearly evidenced in this and later sections.

4. Notable Publications

For each member of staff listed in section 2b above, please provide full (not shortened) web links to electronic versions of up to four notable relevant publications published, or accepted for publication, in the period December 2013 to December 2018 (note that full versions of papers must actually be accessible via the link you provide). For each publication, provide a brief description of:

a) where and when it was published

b) its significance

c) its known impacts

d) its relationship to the areas in Knowledge domains relevant to this scheme.

Criteria to be applied

Publications are an indicator of the quality of the research being undertaken by your organisation. There should be an active publication and influencing culture within the organisation, producing clear evidence of relevant, high quality outputs that have had an impact within and beyond the research community.

Collaboration within your organisation is taken as a sign of a healthy environment, although our experience of previous calls is that multiple citations of the same work by different named staff will not add significantly to the case for recognition. Similarly, the panel is unlikely to include a project in its consideration unless the relevance of the work undertaken is made very clear. Therefore, applicants are strongly advised to include a concise synopsis describing the relevance of the research to cyber security. Publications whilst a member of staff was at a different institution are eligible, provided the member of staff is employed at the institution making the application on the census date of 01 December 2018.

5. Doctoral Level Students Programme

For each doctoral thesis successfully completed at your institution during the period December 2013 to December 2018, please provide the following information:

a) start date

b) end date

c) thesis title

d) aims

e) relevance to technical areas listed in Knowledge domains relevant to this scheme

f) key outcomes

g) where the student is now (if available)

h) name of supervisor at institution

For each doctoral student who was registered at your institution during the period December 2013 to December 2018 but who has not yet submitted a thesis, please provide the following information:

a) start date

b) topic of research

c) relevance to the technical areas listed in Knowledge domains relevant to this scheme

d) name of supervisor at institution

Please do not provide any personal student information, including names, without their permission.

Criteria to be applied

A vibrant doctoral-level students' programme is an indicator of the health of your organisation's cyber capability and its ability to produce the next generation of researchers. To be recognised your institution will need to have produced a minimum of **ten** successful and directly relevant doctoral theses during this period. The rate of thesis production (number of theses produced per year)

should be reasonably constant over the period or show an increasing rate towards the later years. It should be clear that each completed thesis has made a direct contribution to one or more of the technical areas listed in Knowledge domains relevant to this scheme. A minimum of **ten** demonstrably relevant doctoral students should have started in the same period. The rate of new starts (number of new starts per year) should be reasonably constant over the period or show an increasing rate towards the later years. Students supervised by staff when they were employed by other organisations, and who received degrees from those organisations, should not be included. Students supervised by staff who left your organisation before the census date may be included. These will be viewed in the light of your organisation's continued commitment to maintaining a substantial cyber security capability. Our experience of previous calls is that it is very unlikely that the assessment panel will wish to include a particular thesis in its consideration unless the actual relevance of the specific doctoral work undertaken is made very clear. Therefore, applicants are strongly advised to include of a concise synopsis describing the relevance of the thesis to cyber security; titles rarely suffice.

6. External Research Funding and Impact of Projects

Provide details of all relevant external research funding received during the period December 2013 to December 2018. This should include:

a) name of your organisation's principal investigator

b) name of project

c) start and end dates

d) funding agency

e) for projects including other partner research organisations the actual spending within your organisation

f) whether the award was a result of a competitive process.

In addition, identify up to five of the projects active in this period which are considered to have been particularly successful in terms of the quality of their outputs and their influence in the academic, business, regulatory or government community in cyber security. For each project, briefly describe the key outcomes and impact along with its relationship to the technical areas in Knowledge domains relevant to this scheme. Impact could include things such as: uptake of research results by other academic groups or business; production of software and hardware artefacts that have been made available to the research community; surviving or subsequently acquired spin-out companies formed as a result of the research undertaken.

Criteria to be applied

Relevant external research funding is an indicator of the value, in a broad sense, that others place on your organisation's cyber capabilities. There should be clear evidence of **sustained** research income over the period, from a **diversity** of sources and provided with a **range** of intentions, sufficient to provide **most or all** of the staff named in Section 3 with the resources needed to undertake leading-edge research. (There is no requirement to limit cited funding to the subsequent examples of impact as long as the funding is relevant.) There should

also be clear evidence of your organisation having undertaken relevant research projects with important outputs and identifiable impact. The PI for all projects cited must be a member of staff named in Section 3. Experience shows that the panel is less likely to accept multiple examples of projects whose only or primary impact is in papers produced or number of academic citations; therefore applicants are strongly encouraged to include a variety of impacts.

Knowledge domains relevant to this scheme

This section provides a summary of the research areas that are within scope for Academic Centres of Excellence in Cyber Security Research. To be in scope, research and training in these areas must substantively address and be driven by security needs.

The summary list is not meant to be exhaustive but is meant to cover the majority of research areas that the scheme's sponsors consider essential to ensure the UK's cyber security. Other areas may be included provided that the application provides a sufficiently strong and clear case for their importance and relevance to genuine cyber security issues.

Although the summary list may appear to be technology dominated, please note that the sponsors consider that system security depends not just on technology but also on people and processes. The human and organisational aspects of all the areas listed are, therefore, of equal importance.

Research areas

1. Cryptography, Key Management and Security protocols

This area includes:

- Cryptographic primitives and protocols including quantum-safe cryptography and advanced cryptography (such as identity-based and attribute-based encryption, homomorphic encryption, multiparty computation, zero-knowledge). All aspects of design, analysis, implementation and assurance including formal verification.

- Quantum computing for cryptanalysis and impact of novel computation.

2. Sociotechnical Security

This area is about how humans, processes and technology can work together to improve cybersecurity. Research in this space should explore the tools and techniques that could enable better cyber security practice. This area includes:

- Communicating risk – providing decision makers with targeted, contextualised and accurate information

- Risk frameworks and methods – creating new cyber risk management techniques, or adapting them from other professions, to improve the management of cyber risk across the UK

- System modelling – to explore the wide range of techniques available for representing and addressing cyber security challenges

- Cybercrime – understanding and reducing the harm to victims

- Usable security – understanding how people interact with security, technology and infrastructure in order to optimise design engineering processes

- Organisational factors – topics that emerge from individual and group behaviour and structures; in a team, organisational or societal level

- Discovery – the elicitation of ground truth to inform people-centric cyber security approaches

- Privacy.

3. Hardware Engineering

This area includes:

- Hardware security and anti-tamper techniques, including for printed circuit boards (PCB), application-specific integrated circuits (ASIC), field-programmable gate arrays (FPGA), System-on-chip, memory devices, and microprocessor technologies

- Hardware vulnerabilities and countermeasures, including fault detection mechanisms, supply chain vulnerabilities, and counterfeit detection and prevention

- Physics of semiconductors devices and post-silicon electronics, including memory technologies, hardware noise sources, and circuit primitives

4. Total Network Defence

This area includes:

- Developing new ways to detect, classify and defend an entire network against malicious activity, by combining data from several sources such as: network captures; firewall activity; virtual machine images; host-based sensors; system configuration and log files; active scans

- Development of new techniques that can be used at national scale to have a significant impact on uplifting cyber security

- Furthering the cutting edge in practical security monitoring, making it easier and cheaper to do a good job of identifying compromises

- Ways to develop a better understanding of what technology organisations actually have, since many breaches seemingly exploit systems or technologies that organisations did not realise they had.

5. Strategic Technologies and Products

This area includes:

- Development or assessment of mitigation technologies in hardware and software platforms. How vulnerabilities are mitigated effectively today and how they might be mitigated in the future in a standard mobile or desktop computer

- Research addressing the quality and development of mitigation technologies across the range of platforms available today to consumers. This could consider how they are bypassed today and historically.

- Novel options for exploit mitigates and defences against the most prevalent vulnerability classes.

- Research into the quality, prevalence, variation and utilisation of mitigation/safety features in coding platforms, especially given the uplift in new languages

- Data and service architectures – the intersection of safety and cyber security. How we can design systems which can be maintained from a security perspective whilst not undermining confidence in their safety characteristics. How computer systems can be maintained to remain both safe and secure.

These objectives might be met through the use of the following (note this list is not exhaustive):

- Technologies, including: General Purpose Operating Systems, General Purpose Applications, Processors and Architectures, Embedded Devices, Inter-Device Communications, Virtualisation and Emulation, Web technologies, Roots of Trust, Trust Infrastructure, Network Functions Virtualisation, Software Defined Networks

- Methodologies, including: Dynamic Analysis, Static Analysis applied to hardware, software, systems and/or networks

- Data and Service Architectures, including: Enterprise IT, Online Services, Cross Domain Solutions, Control Systems, Shared Services/Cloud, Telecommunications Systems

- Identity Assurance, including: biometrics; identity systems and technologies; biometrics vulnerabilities; transactional security; mobile money; online service access; PKI; RFID; Smartcards; soft credentials, passwords and PINS; identity federation; behaviour, device and location metrics; data anonymisation.

6. Side Channel and Fault Analysis

This area includes:

- Electromagnetic Physics and Security, including: transmission and propagation modelling; TEMPEST measurement and testing; and understanding of technology-specific emissions

- Power/Electromagnetic Side Channel Analysis, including: leakage detection and modelling; analytical tools and techniques; countermeasure design; modelling countermeasure behaviour; implementation-aware security proofs; and measurement and testing systems

- Microarchitectural Side Channel Analysis, including: leakage detection and modelling; analytical tools and techniques; countermeasure design; modelling countermeasure behaviour; implementation-aware security proofs; and measurement and testing systems

- Fault analysis, including: fault modelling in practical injection systems; fault-based cryptanalysis; algorithmic countermeasures.

7. Building trusted and trustworthy systems

This area includes:

- Understanding how expert security architects find architectural flaws in systems and make judgements of overall system security, with a view to better describing and formalising some of the techniques they use so assessments can be more repeatable and new security architects can be developed faster

- Development of new architectural principles and patterns to help system designers solve common problems, including the development of more modern patterns to overcome the shortcomings of long-established patterns

- Development of alternate system architectures to better manage security risk in some of the hardest system design challenges, such as (not an exhaustive list):

    - Deploying extremely sensitive or high value workloads into the public cloud whilst having supreme confidence that the data remains secure from rogue insiders within the third party

    - In cloud computing, gaining confidence in the integrity of the host when you can only run code on the guest

    - The modernisation of crypt key distribution for sovereign applications

    - Taking the 'bulk' out of bulk personal data breaches

    - Importing untrusted data into systems that need to maintain the highest levels of integrity and confidentiality

    - Exporting specific content from systems that contain very sensitive data, without allowing the inadvertent or deliberate leaking of other data

    - Allowing third party access to parts of a high integrity control system, without undermining security of the system

    - Enabling software developers to have the flexibility they desire from their development device without undermining the security of the system they are developing code for, in the event their device is compromised

- Identification of disparities between the system that was designed and the system that was built

8. Security of Critical Systems and Operational Technology

This area includes:

- Risk management approaches and application to critical systems, understanding dependencies, determining criticality
- Interventions from the hardware up to government policy. Novel options for intervention, comparing differing interventions, measuring effectiveness
- Detecting intrusion in systems providing critical services, including bespoke and embedded systems
- Incident response and forensics for critical systems, including bespoke and embedded systems
- Understanding obstacles to perceived best practice being applied to systems providing critical services.

Assessment

Assessment process

Applications will be assessed by an Assessment Panel which will include representatives from government, business and academia. Each application will be read and scored independently by a minimum of three members of the Assessment Panel. At the Assessment Panel meeting, Panel members will present their scores and the rationale for their scores.

Each application must include document 1) (Institution's Letter of Support) – without it, the application will be rejected as non-compliant.

Sections 2) to 6) of each application will be scored using the following scale:

1) no evidence
2) very little evidence
3) partial evidence
4) good evidence
5) excellent evidence

Each of the sections 2 to 6 must achieve a threshold score of 3. If the application includes a letter of support and the consensus score is at threshold or above in each of sections 2 to 6 then the application will be deemed to be successful overall.

The Assessment Panel will agree a consensus score for each application against each criterion and so make a recommendation on whether or not to recognise an applicant organisation as an ACE-CSR. There is no pre-defined upper limit on the number of ACEs-CSR that might be recognised.

Assessment criteria

The detailed assessment criteria and some further advice based on our experience of earlier calls are defined in the section 'Required Structure of Application'.

To be successful, applications must meet or exceed the minimum scoring threshold in all five assessment areas:

- Research environment and strategy
- Track record and esteem indicators for members of staff
- Notable publications
- Doctoral level students programme
- External funding and impact of projects

The assessment areas are all equally weighted.

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/

Moving forward

You will be notified of the result as soon as possible following on from the assessment panel. Feedback based on the panel's discussions will be made available to all applicants.

You will need to submit a separate application through Je-S for the EPSRC support grant. Further details of this process are available in Annex A of this document.

Submissions to this call will not 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/

All information you provide will be treated confidentially and not shared by EPSRC or the NCSC except for the purposes of this assessment process (though see 'Further use of information in applications' below.)

Further use of information in applications

We expect the applications received in response to this call to contain much valuable insight and information on the current UK academic cyber research capability. As a result, the UK Government would like to be able to further use the contents of applications received in response to this call to help inform the development of its Cyber Security policies and strategies. **The submission form on the call webpage includes a consent tick box for applicants to indicate whether they are happy for the information in their application to be used for this additional purpose.** The ACE-CSR assessment panel will not be made aware of your decision either way. If you agree to re-use, the information will not be used in a way that allows individual institutions or researchers to be identified.

Key dates

Activity	Date*
Call opens	30 January 2019
Deadline for applications	16:00, 26 April 2019
Assessment panel	June 2019
Decision communicated	Week beginning 24 June 2019
Recognition start date	01 July 2019, for three years

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

Contacts

For all enquiries please contact Miriam Dowle at miriam.dowle@epsrc.ukri.org.

Change log

Name	Date	Version	Change
Anna Walker	19/12/18	0.1	Document created
Miriam Dowle	28/01/18	0.2	

Appendix A

EPSRC is able to provide each organisation recognised in the 2019 round as being an 'Academic Centre of Excellence in Cyber Security Research' a grant of £60k (the 100% fEC cost, meaning that the maximum EPSRC contribution will be £48k) over its expected three-year lifetime. This annex covers the process for requesting these funds.

1. The ACE support grant will be issued as a grant from EPSRC, managed and governed by EPSRC grant terms and conditions. It is not associated with or governed by terms of any other sponsors of the ACE scheme. It is entirely separate from the Terms and Conditions for Membership of the ACE Scheme.

2. Any institution which is recognised as an ACE can submit a request for support funding.

3. It is not compulsory that submitting institutions request the support grant though you should note that all current ACEs have such a grant.

4. The person submitting the ACE application, or otherwise indicated as being the lead contact for the ACE, should normally also be the PI on the support grant application (although this is not a strict rule.)

5. The maximum grant value that can be requested is £60k (100% fEC cost, meaning that the EPSRC contribution will be £48k.)

6. Grants less than this maximum value can be requested.

7. Grants should be requested which cover the expected three-year lifetime of the ACE. In the event that ACE status is lost before its natural end the support grant is likely to be terminated also.

8. As ACE status is given at an institutional level and is unique to that institution, the grant must only feature investigators from the ACE institution.

9. Once awarded, ACEs are allowed and encouraged to share their support resources if appropriate (for example to host a significant ACE networking event involving more than one ACE.)

10. Only researchers named in the ACE application can be investigators on the support grant.

11. All of the guidance on eligibility of investigators found in the EPSRC funding guide applies.

12. Given the restricted level of overall Investigator time allowed (see point 14 below) it is unlikely that there is a case to be made for having any Co-Investigators.

13. In general the ACE support grant can only be used to meet reasonable costs incurred directly as a result of recognition by the sponsors as an ACE. We will try to be flexible while strongly discouraging attempts to

ascribe to the ACE costs which are in reality incurred with other intentions in mind.

14. Among other things, the ACE grant can be used to support:

    a. Development, hosting and maintenance of a dedicated ACE website which describes the composition, expertise and activities of the ACE
    b. Secretarial support for management of activities specifically connected with ACE status
    c. Development and production of publicity materials and activities specifically connected with ACE status
    d. Travel costs associated with attendance at the annual ACE conference and/or other meetings requested by the sponsors
    e. Events which publicise/promote/engage the ACE with users from business or the public sector (these are strongly encouraged)
    f. A reasonable level of Investigator time to coordinate the ACE within the intentions of the scheme and in the spirit of the 'Institution's Letter of Support' submitted as part of the ACE application. Note that a request for some level of Investigator time will be essential to fill in the form. This may be a nominal amount if desired.

15. The ACE support grant can not be used to support:

    a. Any costs not specifically, directly and wholly associated with ACE status
    b. Equipment purchases of any kind
    c. Laptops/desktops/standard printing materials or other consumables normally expected to be found in a university
    d. Infrastructure support costs other than those requested as Estates/Indirect Costs associated with Investigator or Directly Incurred staff.
    e. Anything already indicated as being an institutional contribution to the aims of the ACE in the 'Institution's Letter of Support' submitted as part of the ACE application.
    f. Conference attendance unless specifically with the purpose of promoting the capability of the ACE. Requests for conference attendance using the ACE support grant must be agreed with the sponsors (EPSRC and NCSC in the first instance) in advance. This will be managed through the appointed contacts in EPSRC and NCSC
    g. Research, or support of existing or new research staff
    h. PhD or Masters-level training, in the form of stipends, fees or consumables.

16. These inclusions and exclusions are not exhaustive and may be changed in light of feedback. Any proposals not reflecting them may be altered before announcement or rejected.

17. Proposals should be submitted as 'Standard Research' proposals to EPSRC through a specific call which will be set up in the Je-S system.The title of the call will be "Academic Centres of Excellence in Cyber Security – 2019".

18. The call will open on Je-S from 28 February 2019 and close on 30 April 2019.

19. You will need to prepare and submit your proposal through JeS by the deadline above. We will inform you of the outcome of your application as soon as possible following the assessment panel. If you are not successful, your proposal will be rejected. This will not be counted towards the repeatedly unsuccessful applicants policy.

20. Proposals should follow the standard format and include all of the document types necessary for a Standard Research proposal: Je-S Form, Case for Support, Workplan, Justification for Resources and Impact Plan. Letters of Support are not necessary and CVs for named researchers should not be attached as these are not relevant. There is more information in the checklist at the end of this document.

21. While all the normal document types should be submitted and completed adequately you do not need to provide the full level of detail expected in a normal research proposal. For instance there is no need to use the full six pages to make a case for support.

22. To save time you can and should use the material generated in the ACE application to complete the support proposal wherever possible.

23. If funded, the summary you provide in the Je-S form will appear on EPSRC's grants on the web so please make sure that it makes sense and promotes the ACE to an external audience as effectively as possible.

24. Grants should have the title 'Academic Centre of Excellence in Cyber Security Research – [INSTITUTION NAME]'

25. Please select the Discipline 'Computer Science'

26. The requested start date for the support grant should be 1/7/2019 and the duration 36 months, end date 30/6/2022. Grants will be announced by the end of July 2019 but may not start until the T&Cs are signed. As with all EPSRC grants, costs can be incurred from the date of the offer letter and paid retrospectively if required.

27. Award of the grant will be automatic on recommendation by the panel that ACE status is granted to the HEI.

28. You should not need to do anything post submission of the application other than the standard acceptance process (if successful.)

Attachments Check List for Je-S proposal

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	Not required	
Project Partner Letters of Support	No page limits	Not required	
Letters of Support	No page limits	Not required	
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	Not required	

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.