National Cyber Security Centre
a part of GCHQ

Engineering and Physical Sciences Research Council

Academic Centres of Excellence in Cyber Security Research

Call for Applications

Closing Date for Applications: Wednesday 27th September 2023, 16:00

Deadline for Expressions of Interest: Tuesday 25th July 2023, 16:00

Table of contents

1 Background

During 2011 – 2012, government established a programme to recognise Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). The primary motivation for setting up the ACEs-CSR was to identify excellent university cyber security research and to help establish a cyber security research community across academia, government and industry. A decade on, government believes that the ACE-CSR programme has brought about considerable added value. 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.

2 Aims and benefits of the ACE-CSR programme

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 the CyBOK[1]. 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 level. 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.

The scheme makes collaboration and knowledge exchange 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.

3 Eligibility

This call for applications is open to all UK HEIs. ACE-CSR recognition is given at an institutional level and NCSC will only accept one application from any institution.

[1] https://www.cybok.org/knowledgebase1_1/

4 How to apply

4.1 Expressions of interest

To help the NCSC plan for assessments, all HEIs intending to apply for ACE-CSR recognition must submit an expression of interest (EOI) to academia@ncsc.gov.uk by the deadline of 16:00 on Tuesday 25th July 2023. The NCSC will confirm receipt of EOIs by email.

4.2 Submitting applications

Applications should be emailed to academia@ncsc.gov.uk by 16:00 on Wednesday 27th September 2023. The NCSC will email applicants to confirm receipt of applications. Applicants are solely responsible for ensuring that any application that they submit reaches NCSC and for all costs related to the preparation of their applications.

Nothing in this call for applications document, including any documents annexed to it or otherwise made available (including information or statements made verbally) as part of the application process, shall constitute a contract between the NCSC and applicants or potential applicants (whether express or implied).

4.3 Guidance on writing applications

Applicants should read the application evidence requirements and criteria in section 4.5 carefully when compiling their applications. Your application should be based on evidence (e.g., permanent members of staff) that is correct on the Census Date of 30th June 2023.

Applications should be in PDF format with font size no smaller than 10pt. Please ensure that the file name of all documents submitted includes the name of the applicant's HEI.

Applicants will be solely responsible for the content and accuracy of their applications. Any 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 can be 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.

4.4 Required structure of application

Applications should be structured into the following six sections. These can either be submitted as individual documents or as a single document. If submitting as a single document, please ensure that all sections are clearly marked.

1. **Institution's Letter of Support for Application** (maximum one side of A4)
2. **Case for Recognition** (maximum three sides of A4, plus a completed CyBOK expertise mapping template (provided))
3. **Track Record and Experience of Members of Staff** (maximum two sides of A4 per CV)
4. **Skills and People Development** (section 4.i – maximum two sides of A4; section 4.ii - no word limit but please only include requested information)
5. **External Research Funding and Impact of Projects** (maximum three sides of A4)
6. **Knowledge Exchange and Partnerships** (maximum two sides of A4)

4.5 Evidence required & criteria to be applied

Under each section of the application, please provide the requested evidence to demonstrate how you meet the requirement. For sections 2-6, the criteria against which the evidence will be assessed are described below.

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. In your case for recognition, please ensure that you include sufficient 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 five 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 academic staff[2]. Post-doctoral researchers at Senior Research Associate level (or equivalent) may also be included in the submission. However, to be suitable for inclusion, both permanent and 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 30th June 2023.

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, and any relevant facilities, laboratories, etc.

[2] *Note: We recognise that 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.*

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

e) A synopsis of the research expertise of members of staff named in 2b above in the form of a CyBOK expertise mapping matrix (Excel template provided). Please enter the names of each member of staff into the template and select the appropriate expertise level from the drop-down menu for each CyBOK knowledge area (KA). 'Good' means that the staff member can successfully teach material and supervise dissertations at Master's level in the KA; 'Expert' is a track record of publishing research in the KA. Any blank entries will be interpreted as 'none'.

Criteria to be applied:

- An established, cohesive, integrated and relevant cyber security research programme with a clear strategy and vision is in place.

- The HEI has a minimum of five permanent or long fixed-term, named members of staff who demonstrate a track record of, and potential for future, working collaboratively in areas which are relevant to recognisable significant challenges in cyber security.

- The technical areas to which each member of research staff contributes (whether fully or partially) are clearly mapped to the CyBOK framework using the template provided.

3. Track Record and Experience of Members of Staff

Please provide a CV[3] 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 indicators of experience such as: journal editorship, programme committee membership, invited talks, membership of working groups or advisory groups, and Fellowship of professional bodies or learned societies.

Criteria to be applied:

- The CVs 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 is consistent with the CyBOK expertise mapping template completed for section 2 'Case for recognition'.

[3] *Note: 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. Skills and People Development

i. Skills development

Please describe how the skills of the researchers involved in the department are developed and how researchers are supported during the transition across career stages. You should include example pathways of previous post-doctoral researchers. Please also describe any steps your institution has taken to promote a more diverse, fair and inclusive research environment.

ii. Doctoral programme[4]

For ten (10) of the doctoral theses successfully completed at your institution during the period June 2018 to June 2023, please provide the following information: a) start date b) end date c) thesis title d) aims e) relevance to technical areas listed in CyBOK and/or NCSC Research Problem Book[5] f) key outcomes g) where the student is now (if available) h) name of supervisor at institution.

And, for ten (10) of the doctoral students who were registered at your institution during the period June 2018 to June 2023 but who have 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 CyBOK and/or NCSC Research Problem Book d) name of supervisor at institution. Please do not provide any personal student information, including names, without their permission.

Criteria to be applied

- Post-doctoral researchers and research staff are well supported with career and skills development.
- A healthy number of high quality and directly relevant doctoral theses have been produced during the period June 2018 to June 2023. A similarly healthy number of relevant doctoral students have started in the same period.
- Each completed thesis has made a direct contribution to one or more of the technical areas listed in CyBOK and/or the NCSC Research Problem Book.

5. External Research Funding and Impact of Projects

Please provide details of all relevant external research funding received during the 5-year period ending June 2023. This should include: a) name of your organisation's Principal Investigator (who must be one of the people named in Section 3) b) name of project c) start and end dates d) funding

[4] *Note: 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.*

[5] https://www.ncsc.gov.uk/information/the-ncsc-research-problem-book. *The problem book will be refreshed during 2023.*

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 the CyBOK framework. 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

- The HEI has a 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 of the application with the resources needed to undertake leading-edge research.
- A broad range of relevant research projects with important outputs and identifiable impact, across a range of impact types have been undertaken.

6. Knowledge Exchange and Partnerships

Please provide details of the organisation’s current knowledge exchange activities, including any key partnerships with other academic institutions, government and industry, which are relevant to cyber security research. These can include both funded and non-funded activities, commercial and non-commercial relationships. You should also describe how these activities support and contribute to the strategy and vision of the organisation in relation to developing its cyber security capability, as described in section 2 ‘Case for Recognition’. The outputs and benefits of the activities should be clearly identified.

Criteria to be applied

- A range of collaboration and knowledge exchange activities with external partners (including other academic institutions, government and industry) for the wider benefit of the economy and society, aligned with the strategy of the organisation, are in progress.
- The outputs and benefits of the activities described are clearly defined.

4.6 Points of clarification

This call document, the CyBOK expertise mapping template and a list of any points of clarification regarding the application process will be maintained at https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research.

Applicants are advised to check this web page regularly for any updates to the application process or changes to this call document, such changes to be made at the absolute discretion of the NCSC and without notice.

Applicants are welcome to contact the NCSC before Tuesday 25th July 2023 to discuss any questions or areas of concern they might have. Please contact the NCSC at academia@ncsc.gov.uk.

5 Assessment

Applications within scope will be assessed by a panel that will include, for example, representatives from government, industry and academia. Each application will be read and graded independently by a minimum of three members of the assessment panel.

5.1 Assessment process

At the Assessment Panel meeting, panel members will present their scores and the rationale for their scores.

Each application must include the Institution's Letter of Support (section 1) – without it, the application will be rejected as non-compliant. Sections 2 to 6 of each application will be scored using the following scale:

A – strong evidence provided; criteria fully met

B – fair evidence provided; criteria partially met

C – no evidence provided; criteria not met

The threshold score for each section is A.

If the application includes a letter of support and the consensus score is at threshold 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 HEI as an ACE-CSR.

The panel's decision is final. There is no pre-defined upper limit on the number of ACEs-CSR that might be recognised.

5.2 Notification of result

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.

5.3 Successful applications

Successful applicants will be recognised as an 'Academic Centre of Excellence in Cyber Security Research' by the NCSC and EPSRC for a period of five years, subject to the HEI agreeing the licence terms for use of the ACE-CSR logo. After the five-year period, it is anticipated that a HEI will need to submit a new application in order to renew its ACE-CSR recognition.

5.4 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 NCSC Academia team will contact you following submission of an application to ask whether you are happy for the information in your 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.

5.5 Key dates

Activity	Proposed Date
Call issued	Wednesday 28th June 2023
Deadline for expressions of interest	Tuesday 25th July 2023, 16:00
Deadline for submission of applications	Wednesday 27th September 2023, 16:00
Assessment panel	October/November 2023
Announcement of results / recognition start date	November 2023