Scheme to Recognise Academic Centres of Excellence in Cyber Security Research

Call type: Invitation for Applications

Closing date: 16 December 2011, 16:00

Briefing meeting date[1]: 15 November 2011

Summary

The Government Communications Headquarters (GCHQ) in Cheltenham and the Engineering and Physical Sciences Research Council (EPSRC) intend to set up a Scheme to recognise UK Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). Although the Scheme will initially be run by GCHQ and EPSRC, the vision is that it will achieve support across government and business. This call document sets out the process and requirements for Higher Education Institutions to submit applications to be considered for ACE-CSR recognition.

Important initial objectives of the Scheme are to identify those institutions whose Cyber Security research is excellent and identify those technical areas in which UK research is very strong. This should also help determine research areas that need to be strengthened.

A key element of the Scheme vision is that it will assist government and business to interact more effectively with the university sector both to gain insight into leading-edge university Cyber Security research and to help exploit it for the benefit of the UK. Similarly, the Scheme will provide researchers at ACEs-CSR with better understanding of the range of Cyber Security problems faced by government and business. Longer term, the Scheme should help shape future Cyber Security research requirements and provide a stimulus to enhance the quality and breadth of UK academic Cyber Security research.

Background

Cyber Security

The National Cyber Security Strategy [www.science.mod.uk/controls/getpdf.pdf?141] describes Cyber Space as encompassing all forms of networked digital activity, with Cyber Security concerning all aspects of national security as they relate to Cyber Space. Cyber

[1] Please email cybersecurity@epsrc.ac.uk by 8 November to register intent to attend this meeting, to be held at the Institute of Physics, London

Space is a key enabler for the UK and therefore a critical asset. In the National Security Strategy [http://www.direct.gov.uk/nationalsecuritystrategy] "Hostile attacks upon UK Cyber Space by other states and large scale crime" are considered to be a Tier 1 risk. Tier 1 risks are those with the "highest priority for UK national security, taking account of likelihood and impact." The National Security Strategy effectively states that measures need to be put in place to reduce the risk and impact of such attacks, i.e., the UK needs to defend itself in Cyber Space.

A recent Green Paper from Research Councils UK (RCUK) states that RCUK has identified research into Cyber Security as a priority for its Global Uncertainties programme with the aim of working with academic researchers, businesses and government users to develop activities and opportunities for carrying out world-class research into Cyber Security [http://www.globaluncertainties.org.uk/globaluncertainties/research/Cybersecurity-green-paper.aspx]. RCUK envisages that Cyber Security research will contribute to making the UK a safer place to live and work, helping to make it an attractive place to invest. RCUK encourages Cyber Security research that crosses discipline boundaries, especially recognising the importance of bringing together technological and people-centred expertise from across the remits of the Research Councils.

Cyber Defence is a sub-set of Cyber Security that includes all activities undertaken to reduce the risks to, and impacts on, UK Cyber Space that may arise from threats within, and external to, UK Cyber Space. Cyber Defence is about defending the UK's Cyber Space. In the context of Cyber Defence, Information Assurance is a key discipline that enables organisations to manage risks to their own Cyber Security and reduce the harm from a variety of threat actors, including those residing in Cyber Space.

The focus of this Scheme is Cyber Security research being undertaken at UK universities that is contributing to the goal of Cyber Defence. Thus, throughout the remainder of this document references to Cyber Security should be taken as being synonymous with Cyber Defence.

Aims, Vision and Benefits of the Scheme

The overall aim of the Scheme is to identify and recognise eligible research organisations that are carrying out cutting-edge Cyber Security research in one or more of the technical areas (set out in Appendix A) that underpin Cyber Security. Although the Scheme will initially be run by GCHQ and EPSRC, the vision is that it will achieve support across government and the business community.

An important initial objective of the Scheme is to identify the set of UK institutions whose Cyber Security Research is excellent. This will highlight areas where there is critical mass, impact and research excellence. It may also help identify areas where there are technical gaps and provide evidence upon which to base future research priorities.

A key part of the Scheme vision is that it will help facilitate ACEs-CSR, government and business to work together and share knowledge. It is hoped that it will enable government and business interact more efficiently and effectively with the university sector and gain a deeper understanding of leading-edge academic research that could be harnessed for UK Cyber Security.

Similarly, academic researchers from ACEs-CSR should gain better insight into the range of Cyber Security problems faced by government and business. Overall, it is anticipated that the Scheme will provide a basis for the better exploitation of current leading-edge research and the identification of the research needed to ensure the UK is well prepared to meet future Cyber Security challenges and threats.

It is hoped that the Scheme criteria will provide a useful benchmark for the academic community at large and for the set of institutions achieving ACE-CSR recognition to grow in number over the coming years, reflecting improvements to the quality and breadth of Cyber Security research being undertaken. ACE-CSR status should lead to a heightened profile and recognition of an institution's Cyber Security research efforts among peers, government and business.

It is expected that ACEs-CSR would work closely with government stakeholders. To help facilitate effective interactions, any ACE-CSR that is appointed would have a senior technical person from GCHQ or another government stakeholder organisation assigned as a liaison officer.

It is anticipated that there would be an annual conference to which representatives from ACEs-CSR, government and business will be invited. In addition, there may be opportunities for collaboration with other Academic Centres of Excellence overseas.

An Institution whose submission is successful would be able to hold the title of 'Academic Centre of Excellence in Cyber Security Research' for a period of 5 years, subject to complying with appropriate terms and conditions of membership of the Scheme. It is intended that a draft of these terms and conditions will be issued before the briefing meeting on 15 November 2011.

Potential applicants should note that there will be no direct funding associated with ACE-CSR recognition.

Research needs within the Scheme

Addressing the challenges of Cyber Security requires a broad spectrum of world-leading research. For example, research is needed in areas that are relatively well established such as cryptography, as well as relatively newer topics such as malware analysis and intrusion detection. Moreover, it is vital that areas that have traditionally not been core elements, such as human factors and economics, should play a key role in the UK's future Cyber Security research activities. Appendix A provides an indicative list of relevant research areas.

Requirements for Recognition as a ACE-CSR

The specific criteria that institutions have to meet in order to be recognised as ACEs-CSR are set out in Appendix B. An institution whose submission meets or exceeds the threshold in all of the criteria will be eligible to be recognised by GCHQ and EPSRC as an Academic Centre of Excellence in Cyber Security Research. There is no pre-defined upper limit on the number of ACEs-CSR that might be recognised.

In order to be recognised as an ACE-CSR, an institution will need to demonstrate critical mass and excellence in its Cyber Security research and provide good evidence of:

i. An active, cohesive, integrated and effective Cyber Security research environment, with a clear focus and a clear future strategy and vision.

ii. Members of staff who are active, have a demonstrable track record in Cyber Security research, who work together effectively and who are recognised and influential in research communities and those communities that fund research and make use of research outputs.

iii. High quality peer reviewed publications that are recognised by the research community at large.

iv. An active and sustained Doctoral Level student programme.

v. Sustained and sustainable external research funding together with projects having clear outcomes and impact.

Eligibility

Higher education institutions and some research council institutes and independent research organisations can request recognition as an ACE-CSR. A list of organisations eligible to apply for this opportunity is provided at: http://www.rcuk.ac.uk/research/Pages/Eligibilityforrcs.aspx.

Institutions will be responsible for checking whether they are eligible to be recognised as an ACE-CSR and neither EPSRC nor GCHQ accepts any responsibility for the costs of ineligible submissions that may be submitted.

There is no funding associated with ACE-CSR status, however recognition as an ACE-CSR will mark an institution out as having met a set of criteria specifically designed to recognise high-quality work in Cyber Security Research.

ACE-CSR status will be recognised 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 be rejected.

How to apply

Submitting application

Applications should be emailed to cybersecurity@epsrc.ac.uk by 16:00 on 16 December 2011.

Guidance on writing application

Applicants will be solely responsible for the content of their applications, however they should note that applications should follow the structure shown in Appendix B.

A briefing meeting is planned for potential applicants on the afternoon of 15 November 2011 at the Institute of Physics in London. Please email cybersecurity@epsrc.ac.uk by 8 November to register intent to attend.

Assessment

Assessment process

Applications will be assessed by an Assessment Panel which will include representatives from EPSRC, GCHQ, government, business and academia. Each

application will be assessed against the set of criteria shown in Appendix B. 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. The Assessment Panel will agree a consensus score for each application.
To be successful, applications must meet, or exceed, the minimum (scoring) threshold in all five areas:

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

Assessment criteria

The detailed criteria are presented in Appendix B.

Moving forward

It is expected that applicants will be notified of the outcome of their application by 31 March 2012.

It is anticipated that there will further calls for ACEs-CSR in October 2012, October 2013 and October 2014. Applications which are not successful in this initial round will be given feedback and, where appropriate, such applicants will be encouraged to submit in future rounds.

Key dates

Activity	**Date**
Register intent to attend briefing meeting. Send email to cybersecurity@epsrc.ac.uk.	8 November 2011
Briefing meeting at the Institute of Physics, London. It is intended that the Draft Terms and Conditions for ACE-CSR Membership will be made available on or before the briefing meeting.	15 November 2011 (afternoon)
Applications due.	16 December 2011
Assessment of applications.	January to March 2012
Expected notification of results sent to applicant institutions.	31 March 2012

Contacts

If you have any questions about this ACEs-CSR Scheme please contact:

Alex Hulkes
EPSRC
Polaris House
North Star Avenue
Swindon
SN2 1ET

Email: alex.hulkes@epsrc.ac.uk

Appendix A: Cyber Security Research Areas

This Appendix 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 in these areas must substantively address security, not merely be using it as an example, nor having a sole focus elsewhere such as, by way of example, on safety.

The summary list is not meant to be exhaustive, but is meant to cover the majority of research areas that GCHQ and EPSRC consider essential to ensure the UK's Cyber Security. Other areas will be accepted by GCHQ and EPSRC provided that the application provides a sufficiently strong and clear case.

Although the summary list may appear to be technology dominated, it should be noted that GCHQ and EPSRC consider that system security depends not just on technology but also on people and processes. Applications should include evidence from across academic disciplines where possible.

Cryptography, Key Management and Related Protocols

This area includes:

- Cryptographic Research
- Quantum Cryptography
- Key Management
- Applied Cryptography
- Authentication Protocols
- Provable Security

Information Risk Management

This area includes:

- Threat Assessment
- Information Risk Assessment and Analysis Methods
- Information Risk Decision Process
- Business Impact
- Information Risk Mitigation
- Information Risk Governance

Systems Engineering and Security Analysis

This area includes:

- Research into methodologies for engineering end to end systems
- High Assurance Software
- The Hardware-Software Boundary, including virtualisation and trusted platforms
- Access Control
- Software Engineering Techniques
- Electromagnetic Security
- Side Channel Attacks and Countermeasures
- Embedded Security
- System on Chip, FPGA and ASIC design of cryptographic algorithms
- Anti-tamper
- Reverse Engineering
- Secure Sanitisation
- Hardware Development Techniques – for example, the use of COTS in secure products

Information Assurance Methodologies

This area includes:

- Techniques for gaining confidence in software/hardware implementations of security controls
- Measuring the effectiveness of combining different security controls in a system
- Large-scale analysis of complex systems for design and implementation faults
- Static and dynamic analysis of products and systems
- Combining and targeting assurance techniques to make risk decisions
- Translating assurance outputs into risk management decisions

Operational Assurance Techniques

This area includes:

- Vulnerability Discovery Techniques
- Intrusion Detection Techniques
- Intrusion Analysis Techniques
- Digital Footprints and Active Defence
- Forensics
- Malware Analysis
- Real-time situational awareness
- Converting situational awareness or attack information into an assessment of the impact on the business
- Vulnerability Analysis
- Intrusion Tolerance Techniques
- Recovery Techniques
- Threat Mitigation

Research into the Security of Technologies and Products

This area includes:

- Communications Technologies and Architectures, for example:
    - Security of Mobile Devices
    - Cloud Security
    - Security of Smart Grid and Smart Metering

- Data and Service Architectures
- Databases and Information Stores
- Web Technologies
- Identity Management
- Steganalysis

Science of Cyber Security

This area includes:

- Measuring Security
- Economics of Security
- Techniques for Assessing Risk and Trust
- Analysing Attacks
- Common Language for Security
- Security Design Principles
- Human Factors – understanding the role of the human in Cyber Security

Building Trusted and Trustworthy Systems

This area includes:

- Formal Methods
- Dependability/Resilience/Survivability against Cyber threats/attacks
- Privacy
- Trust

Appendix B: Required Structure of Application

This appendix provides details of the information that applicants should provide with their application along with the criteria that will be applied.

Each application should comprise six sections, each section submitted in the same email but as a separate document. The documents should be clearly identified under the following headings:

1) 'Institution's Letter of Support for Application' (up to one side of A4).

2) 'Description of the Applicant', which should include details of the research environment, and strategy and vision (up to three sides of A4).

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) 'Peer-Reviewed Publications' (no more than one side of A4 per member of staff, combined into a single document which contains all the necessary Web links to publications).

5) 'Doctoral Level Students Programme' (page limit not specified though please note the requirement for brevity).

6) 'External Research Funding and Impact of Projects' (up to three sides of A4).

Documents should be in Word or pdf format with the font size no smaller than 10pt. Additional documents and information will not be assessed. All information provided will be treated confidentially and used only for the purposes of assessing applications.

In their applications, Applicants should provide evidence (e.g., permanent members of staff) that is correct on the 'Census Date' of 2 December 2011.

1) Institution's Letter of Support for Application

Please provide a signed letter from the Vice Chancellor (or equivalent) showing that the Institution is applying to be considered as part of the Scheme to identify and recognise Academic Centres of Excellence in Cyber Security Research (ACEs-CSR).

Applicants are reminded that ACE-CSR status will be recognised 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 be rejected.

2) Description of the Applicant

Please ensure that you cover the following points:

- The names and structure of the department(s) /group(s) /school(s) making the submission together with the names, seniority and roles of permanent members of staff. (For present purposes, permanent members of staff are those eligible to be Principal Investigators on a Research Council grant [http://www.epsrc.ac.uk/funding/apprev//fundingguide/Pages/defau

lt.aspx].) Also provide the names of Research Assistants (or equivalent) and Visiting Professors.

- A description of the proposed ACE-CSR as it currently stands, including:
    - The areas of Cyber Security Research currently being undertaken.
    - Its development over the past 5 years or so.
    - Facilities, laboratories, etc.
- Recent investments from the Institution, government, business, etc.
- The strategy and vision of the proposed ACE-CSR over the next five years, to include the focus of its research, how it is envisaged that the proposed ACE-CSR will operate and its plans for sustainability and growth.

Criteria to be Applied

The proposed ACE-CSR must have an established, cohesive, integrated and focused Cyber Security research programme. To ensure critical mass, there should be a minimum of 5 permanent members of staff who demonstrate a track record of working together in the areas of the proposed ACE-CSR. There should be a well funded research environment that is well equipped and supported by the Institution. The proposed ACE-CSR must have a clear research focus, strategy and vision.

3) Track Record and Esteem Indicators of Members of Staff

For each of the permanent members of staff named in the application, please provide a CV. The CV should clearly describe academic and other relevant experience, current role, the contribution made to Cyber Security Research within the proposed ACE-CSR, and a list of publications. The CV should also contain esteem indicators such as: journal editorship, programme committee membership, invited talks, membership of working groups or advisory groups, Fellowship of professional bodies or learned societies, or equivalent esteem indicators.

Criteria to be Applied

The CVs should clearly demonstrate that personnel have a proven track record and depth of experience in Cyber Security research and that this is recognised by the research community at large.

4) Peer-Reviewed Publications

For each permanent member of staff, please provide Web links to electronic versions of up to four peer-reviewed publications published, or accepted for publication, in the period January 2007 to December 2011 (note that this should not be a subscription service). For each publication, provide:

- details of where and when it was published
- a brief description of its significance
- known impacts
- its relationship to the technical areas in Appendix A.

Criteria to be Applied

Peer-reviewed publications are an indicator of the quality of the research being undertaken by the proposed ACE-CSR. There should be an active publication culture within the proposed ACE-CSR. There should be clear evidence of relevant, high quality publications that have had an impact within, and beyond, the research community. Collaboration within and beyond the proposed ACE-CSR is essential.

Publications whilst a permanent member of staff was at a different institution are acceptable, provided the member of staff is employed at the institution making the application on the Census Date of 2 December 2011.

5) Doctoral Level Students Programme

For each Doctoral thesis successfully completed during the period January 2007 to December 2011, please provide the following information:

- start date
- end date
- thesis title
- aims
- relevance to technical areas listed in Appendix A
- key outcomes
- where the student is now (if available)
- name of supervisor

For each Doctoral student who was registered during the period January 2007 to December 2011 but who has not successfully submitted his/her thesis, please provide the following information:

- start date
- topic of research
- name of supervisor

Criteria to be Applied

A vibrant Doctoral-level students' programme is an indicator of the health of the proposed ACE-CSR and its ability to provide the next generation of researchers in Cyber Security. There should be an average of two successful theses produced per year and two new Doctoral students starting per year during the above period. It should be clear that each completed thesis has made a scholarly contribution to one or more of the technical areas listed in Appendix A.

6) External Research Funding and Impact of Projects

Provide details of external research funding received during the period January 2007 to December 2011. This should include: name of the Institution's principal investigator; name of project; start and end dates; funding agency; financial

value to the Institution; whether the award was a result of a competitive process.

Identify up to five of the projects active in this period which are considered to have been particularly successful. For each project, describe the key outcomes and impact along with its relationship to the technical areas in Appendix A. 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; spin-out companies formed as a result of the research undertaken.

Criteria to be Applied

External research funding is an indicator of the value, in a broad sense, that others place on the work of the proposed ACE-CSR. There should be clear evidence of sustained research income over the period from a diversity of sources sufficient to provide permanent members of staff in the proposed ACE-CSR with the resources needed to undertake leading-edge research. There should also be clear evidence of the proposed ACE-CSR having undertaken relevant research projects with important outputs and identifiable impact.

Assessment of Applications

Each application will be read and scored independently by a minimum of three members of the Assessment Panel using the criteria above. At the Assessment Panel meeting, the relevant Panel members will present their scores and the rationale for their scores. The Assessment Panel will agree a consensus score for each application.

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:

- 0: no evidence
- 1: very little evidence
- 2: some evidence
- 3 : good evidence
- 4: 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.