Australian Government
Department of Education and Training

Academic Centres of Cyber Security Excellence

Program Guidelines

Open: 22 February 2017

Close: 13 April 2017

Version Control

Date	Version	Description
February 2017	1.0	First release of the ACCSE program guidelines

Table of Contents

1 Introduction

1.1 The Australian Government is committed to enabling security innovation, growth and prosperity for all Australians through strong cyber security. On 21 April 2016, the Government released Australia's Cyber Security Strategy that establishes five themes of action for Australia's cyber security over the next four years to 2020:

- A national cyber partnership
- Strong cyber defences
- Global responsibility and influence
- Growth and innovation
- A cyber smart nation.

1.2 The Academic Centres of Cyber Security Excellence (ACCSE) program has been established to contribute to addressing the fifth theme – A cyber smart Nation. ACCSE will help build Australia's academic and applied capability in all fields of cyber science by bringing together the academic strengths of universities with business, government and other research organisations. The work of these centres will underpin the success of the other four themes under the Cyber Security Strategy.

1.3 The program aligns with the Australian Government's Science and Research Priorities - Cyber Security capability which aims to: *position Australia as a leader in cutting edge cyber security research and innovation to safeguard Australia's security, enhance resilience and enable economic growth.* Australia's Science and Research Priorities identify areas that are of immediate and critical importance to the nation and its place in the world. They help align the nation's education and research to business and government priorities and ensure they capitalise on comparative advantages and address challenges.

1.4 Australia needs to build cyber security capabilities, expertise and understanding to better anticipate, avoid and respond to cyber threats. To achieve this Australia must ensure:

1.4.1 graduates have the right educational opportunities and job ready skills needed to understand and participate in Australian business, government and other institutions

1.4.2 inspire students to think about careers in cyber security and to study science, technology, engineering and mathematics (STEM) subjects

1.4.3 that our leaders and senior managers in government, professional sectors (eg health and education) and business have access to executive education training programs to enhance understanding and increase competence and participation in areas such as cyber security management, legal implications and risk management

1.4.4 that research is collaborative and of national and international significance.

1.5 The Government has committed $1.91 million (indexed) over four years from 2016-17 to 2019-20 for the establishment of academic centres of cyber security excellence.

1.6 The ACCSE program is delivered by the Department of Education and Training.

1.7 These guidelines set out the eligibility requirements, selection criteria, application process and evaluation criteria for the ACCSE program. Applicants should read these guidelines and any related documents carefully before submitting an application for ACCSE funding.

1.8 The ACCSE program guidelines and application form are available on the department's website.

2 Program objectives and outcomes

2.1 The objective of the program is to recognise the significance and ensure the relevance and effectiveness of cyber security programs and professions as part of the Government's Cyber Security Strategy. Academic Centres of Cyber Security Excellence in Australian universities will address the national shortage of highly-skilled cyber security professionals including in technical and non-technical fields as they relate to cyber security.

2.2 The program will help build the nation's capability in cyber security by encouraging more students to undertake studies in cyber security and STEM. It will increase the number of tertiary graduates with the ability to apply their knowledge and skills to the advancement of cyber security capabilities in Australian business and government. It will also broaden the appeal of such careers and broaden the range of professionals capable of supporting a cyber-secure nation into the future.

2.3 The ACCSE program will give recognition to Australian universities that successfully demonstrate high level cyber security education and training competencies, research capability and strong connections to government and the business sector. This applies not only to the provision of cyber security specific qualifications, but also flexibility for students to study cyber security as part of their degree in a broad range of disciplines (eg Schools of Business, Legal, Teaching, Marketing, Engineering, Social studies and others).

2.4 The program will provide some financial support to successful applicants to assist with the establishment ACCSE that will:

- deliver excellent cyber security higher education, training and research, including through specialised courses for undergraduate and postgraduate students
- produce graduates with experience of the cyber security work environment and the skills needed to tackle emerging cyber security challenges in Australian businesses and government
- promote interest in and an understanding of the importance of cyber security to increase the number of people undertaking cyber security study and employment
- undertake research projects that benefit Australia's cyber security
- deliver executive education programs to increase the awareness and capabilities of existing leaders and senior managers who are engaged with cyber security issues in government, business and professional sectors such as education and health
- provide access to cyber security training for non-security and information technology related courses as elective subjects.

2.5 Each ACCSE will be expected to work closely with the Cyber Security Growth Centre (CSGC) to help achieve the expectations in 2.4 (above). The CSGC will provide researchers at ACCSE with opportunities to address priority cyber security challenges and threats faced by government and business.

2.6 Successful applicants will receive recognition as an 'Academic Centre of Cyber Security Excellence'. ACCSE status will assist in raising the profile of the university's capabilities as a high quality institution for cyber security excellence in research, education and training.

2.7 A university will hold the title of 'Academic Centre of Cyber Security Excellence', subject to the project continuously meeting the relevant Conditions of Grant, including milestones and key performance indicators.

2.8 Longer term expected outcomes of the ACCSE program are:

2.8.1 increasing the number of graduates from non-security and information technology related programs with basic knowledge of cyber security and how it relates to their chosen field

2.8.2 increasing the number of skilled cyber security professionals entering the workforce and able to help shape future research and training requirements for our nation

2.8.3 the provision of quality professional executive training for senior managers and leaders in areas relevant to cyber security to increase awareness of cyber security threats, cyber security risk management and inform better cyber security practice

2.8.4 increasing the number of cyber-security professionals from under-represented groups such as women and Indigenous people

2.8.5 research projects that make a valuable contribution to the Australian Government's Cyber Security Strategy and the Science and Research Priorities

2.8.6 increased commercialisation of research outcomes in areas of cyber security.

2.9 Immediate expected outcomes of the ACCSE program are:

2.9.1 an increase in collaboration between universities, business and government in terms of:

a) program design that reflects government and business needs

b) workplace training and mechanisms that support enhanced interaction or exchange between university academics, government and business professionals

2.9.2 an increase in promotional activities that actively stimulate interest in ACCSE undergraduate, postgraduate and professional education and research training programs

2.9.3 an increase in the number of Masters and/or Doctoral internships supported by businesses or other institutes.

2.10 The ACCSE program contributes to Outcome 2.6 Research Capacity of the Department of Education and Training's Portfolio Budget Statements 2016-17:

Research advances our knowledge and drives our potential for innovation, economic competitiveness and social change. The program aims to increase the production, use and awareness of research knowledge and to improve collaboration between government, industry and the research sector in the production of research knowledge.

3 Definition of a 'Centre'

3.1 An ACCSE is a 'Centre' that is assessed as excellent against the selection criteria set out in this guideline. An ACCSE will be led by a single university and demonstrate an organisational structure that brings together undergraduate and postgraduate studies, professional development and research training. It will deliver certified qualifications, course work, research and work ready graduates in the field of cyber security. It will also produce cyber security educated graduates with an understanding of cyber security within a broad range of non-security and information technology related disciplines.

3.2 A centre might be a network of universities, business and research partners. It may be a virtual centre, a centre on a single university campus or located at different schools on a university campus, on different university campuses and/ or include business and research agency premises.

3.3 A university whose application is successful will hold the Australian Government endorsed title of 'Academic Centre of Cyber Security Excellence' and will need to demonstrate its ongoing commitment to, and achievement of, excellence by adhering to the relevant Conditions of Grant.

4 Eligibility

4.1 The ACCSE program is administered under Section 41-10 Item 11(a) of the *Higher Education Support Act 2003* (HESA). Only universities specified in Section 16-15 of HESA (Table A Providers) are eligible to apply. The application must come from a single entity (Table A Provider) acting as the 'Lead Institution'.

4.2 Multiple applications from a single university acting as a Lead Institution will not be accepted.

4.3 Consortia of other education providers and business can participate as ACCSE partners but the Lead Institution must be an eligible institution as defined in these guidelines.

5 Use of Funding

5.1 The program allows for support to be provided for the establishment of several ACCSE should the selection criteria be met.

5.2 Each successful applicant will receive a small grant of assistance to assist with establishment costs, the amount of which will depend on the number of successful candidates and will be the subject of a decision by the Minister for Education and Training.

5.3 ACCSE program funding will be provided to the Lead Institution of each successful application to contribute to activities such as initial set up costs, operational costs including staffing and administration, promotional work and partnerships building support.

5.4 Funds must not be used for:

- any capital works, construction or building activities, including the refitting or upgrade of any existing building
- any purchase, including assets, or other activity for which the Recipient is being provided with other Commonwealth, State or Territory funding.

5.5 Funding will be provided to the Lead Institution under agreed Conditions of Grant. The Conditions of Grant will include key performance indicators, milestones and the project budget. The details of the grant conditions, including payment schedule, will be negotiated with the successful Lead Institution.

5.6 Generally ACCSE funding will be paid in instalments upon completion of the milestones set out in the Conditions of Grant. ACCSE funding will be awarded exclusive of GST.

5.7 ACCSE funding will not duplicate any activity already funded by the Commonwealth or which is likely to be funded from other Commonwealth funding sources. The department reserves the right to determine if an ACCSE project duplicates or is likely to duplicate an activity being funded by another Commonwealth source.

5.8 Program funding for the initiative ceases in 2019-20. It is expected that ACCSE education, training and research programs will become self-sustaining beyond that period.

6 Application process

6.1 There will be one call for applications under the ACCSE program (key indicative dates are outlined under paragraph 11 below).

6.2 The completed ACCSE application form – in Word or PDF format - must be submitted to the department at: accse@education.gov.au by the notified closing date.

6.3 The application must contain a letter of support signed by the university's (Lead Institution) Vice Chancellor. Where an application is for a consortium, all members of the consortium must provide a letter of support to the Lead Institution identifying their commitment to the project.

6.4 Late applications will be considered at the department's discretion only in exceptional circumstances beyond the control of the Lead Institution or partners to the application. The department's decision with respect to late applications will be final.

7 The Application

7.1 In applying for the ACCSE program, the university must provide a plan that demonstrates an integrated strategy to deliver and develop, over the life of the program, a sustainable set of teaching, training and research programs that produce skilled graduates, research excellence and competent cyber security professionals. The plan must demonstrate:

7.1.1 *Degree programs*

a) undergraduate and postgraduate degrees that are cohesive, fully integrated and deliver, cyber-specific skills with pathway options for retaining of graduates in related disciplines

b) opportunities for workplace training and mechanisms that support career pathways in cyber security

c) business mentoring and mechanisms to develop skilled post-graduates (e.g. through internships) for Masters and/or Doctoral students

d) undergraduate and post-graduate enrolments are sustainable and there is a strong completion record and employment outcomes

e) flexibility in terms of making the cyber-security program available (ie as an elective) to a broad range of study disciplines beyond information technology

f) strategies for encouraging under-represented groups, including women and Indigenous people, to undertake studies and pursue careers in the field of cyber security

g) strategies for collaboration with business and a focus on degree programs that develop graduate attributes important to business

h) access to workplace training and mechanisms that support enhanced interaction or exchange between university academics, government and business professionals.

7.1.2 Research programs

a) research programs are in fields of institutional cyber security strength as reflected in Excellence in Research for Australia (ERA) performance and/or enable partnerships with strong utilisation and or potential for commercialisation of outcomes

b) high quality research outputs (eg publications, collaborations, patents, research agreements or contracts) aligned with the Government's Science and Research Priorities - Cyber Security capability

c) engagement of staff with a demonstrable track record in cyber security and a strong standing in this field

d) a track record of, and strategy for, ongoing engagement with government, business or other institutes that fund research and make use of research outputs

e) a track record of commercialisation of research.

7.1.3 Professional programs

a) provision of technical and non-technical training programs designed for professional and executive development training

b) delivery of programs that address market needs – for example cyber/ICT security analysts and architects, forensic examiners and incident handlers

c) availability of courses for developing IT generalists in cyber security (including soft skills, such as negotiation and leadership) to keep pace with the rapidly changing environment.

8 Assessment process

8.1 Applications will be assessed on a competitive basis against the selection criteria at Section 9.

8.2 Applications will be assessed by relevant non-conflicted experts drawn from the Working Group and more broadly as required. Members of the assessment panel will be appointed by the Minister for Education and Training.

8.3 Recommendations will be made to the Minister for Education and Training for approval of successful ACCSE projects, and the amount of funding for each project.

9 Selection criteria

9.1 The following selection criteria will apply in the assessment of applications:

9.1.1 how well the project meets the **program objectives and outcomes as set out in Section 2**

9.1.2 the extent to which the project supports Australia's Cyber Security Strategy theme of A Cyber Smart Nation

9.1.3 the extent to which the project supports the Australian Government's Science and Research Priority Cyber Security capability

9.1.4 how the project supports a cohesive, integrated and effective strategy for the immediate and longer-term sustainability of the ACCSE

9.1.5 the expected outcomes and benefits in terms of research capacity-building in the field of cyber security

9.1.6 the likely effectiveness of the strategy for overall promotion of excellent cyber security research and higher education and training for undergraduate and postgraduate students as well as for professional and executive development, which addresses the needs of business and government

9.1.7 the likely effectiveness of the strategy for supporting an increase in the number of under-represented groups including women and Indigenous people, engaged in cyber-security research, education and training.

10 Conditions of Grant

10.1 Funding will be subject to Conditions of Grant determined by the Minister in writing. These Conditions will define the rights and obligations of the Lead Institution.

10.2 The Conditions of Grant will include, among other things:

- the project aims, approved activities and performance indicators
- total funding and approved project budget
- agreed milestones and associated payments
- reporting requirements, including the frequency of and information required in reports.

10.3 At a minimum, the Lead Institution will be required to submit an annual report on the ACCSE project, setting out:

- expenditure to date
- progress by all parties to the ACCSE towards the achievement of milestones and project outcomes as specified in the Conditions of Grant
- any significant obstacles or challenges.

10.4 All relevant correspondence should be addressed to the delegate of the ACCSE program at:

Branch Manager
Research and Higher Education Infrastructure
Research and Economic Group
Department of Education and Training
GPO Box 9880
CANBERRA ACT 2601

Email: accse@education.gov.au

11 Timeframe

11.1 A summary of key indicative dates is provided below.

Call for applications	22 February 2017
Closing date for applications	13 April 2017
Assessment of applications	Mid-April 2017
Announcement of successful ACCSE	Mid May 2017

12 Freedom of Information

12.1 All documents in the possession of the department with regard to ACCSE are subject to the Freedom of Information Act 1982 (noting that exemptions under that Act may apply to certain categories of documents). Additional information can be found at: https://education.gov.au/freedom-information-0.

13 The Privacy Act 1988

13.1 The department is bound in administering the ACCSE program by the provisions of the *Privacy Act 1988*. Schedule 1 of the Privacy Act contains the Australian Privacy Principles which prescribe the rules for handling personal information. Additional information can be found at https://www.education.gov.au/condensed-privacy-policy.

14 Conflict of Interest

14.1 A conflict of interest arises where a person makes a decision or exercises a power in a way that may be, or may be perceived to be, influenced by either material personal interest (financial or non-financial) or material personal associations.

14.2 Departmental staff are bound by the department's Conflict of Interest and Insider Trading policy available at www.education.gov.au.

14.3 Notified conflicts of interest will be recorded by the department.

15 Further information

15.1 Information on the ACCSE program is available on the department's website.

15.2 Questions about these guidelines should be referred to the Department at: accse@education.gov.au.

16 References

- Australian Government's Cyber Security Strategy https://cybersecuritystrategy.dpmc.gov.au
- Science and Research Priorities, Cyber Security - Capability Statement http://www.science.gov.au/scienceGov/ScienceAndResearchPriorities/Pages/Cybersecurity.aspx
- Australian Information Security Association: The Australian Cyber Security Skills Shortage Study 2016 https://www.aisa.org.au/Public/Training_Pages/Research/AISA%20Cyber%20security%20skills%20shortage%20research.aspx
- Cyber Security Growth Centre www.business.gov.au/cybersecurity
- Australian Research Council – Excellence in Research for Australia http://www.arc.gov.au/excellence-research-australia