Issue 1.0
20 January 2020

Academic Centres of Excellence in Cyber Security Education

Call for Applications

Closing Date for Applications: Thursday 14th May 2020, 16:00

Deadline for Expressions of Interest: Wednesday 22nd April 2020, 16:00

Briefing Sessions for Applicants:

London: Wednesday 12th February 2020

Manchester: Wednesday 26th February 2020

(HEIs thinking of applying are strongly encouraged to attend)

ace-cse@ncsc.gov.uk

Document History

Issue	Date	Comment
Issue 1.0	20 January 2020	First issue

Organisation of this Document

- Section 1: Introduction
- Section 2: Background
- Section 3: Requirements for recognition as an ACE-CSE
- Section 4: Aims and benefits of the ACE-CSE programme
- Section 5: Funding
- Section 6: Eligibility
- Section 7: How to apply
- Section 8: Assessment
- Section 9: Moving forwards
- Appendix A: Required structure of applications for ACE-CSE Gold Award recognition
- Appendix B: Required structure of applications for ACE-CSE Silver Award recognition

1 Introduction

Reflecting the aims of the National Cyber Security Programme, UK Government and its delivery partners are working to increase the UK's academic capability in all fields of Cyber Security. Together the Department for Digital Culture Media and Sport (DCMS), Cabinet Office (CO), UK Research and Innovation (UKRI) and the National Cyber Security Centre (NCSC) have developed a joint approach and strategy for reaching this goal. For example, over the past few years a number of academic programmes have been set up including:

- Academic Centres of Excellence in Cyber Security Research[1]
- Academic Research Institutes in Cyber Security[2]
- Centres for Doctoral Training in Cyber Security Research[3] [4] [5] [6]
- NCSC Certification of Master's, Integrated Master's and Bachelor's degrees in Cyber Security[7]

In the next part of the strategy, the NCSC and DCMS are initiating a new programme to recognise Academic Centres of Excellence in Cyber Security Education (ACEs-CSE) at UK Higher Education Institutions (HEIs).

It should be noted that postgraduate research training (e.g., MRes, MSc by research, PhD, DPhil, EngD, etc.) does not form part of the ACE-CSE assessment criteria.

This call for applications is open to all UK HEIs that on the census date of Wednesday 1st April 2020 have at least one NCSC-certified cyber security degree with Full or Provisional certification at Bachelor's, Integrated Master's or postgraduate Master's level.

Although an HEI with a Provisionally certified degree may apply, please note that ACE-CSE recognition requires the achievement of Full certification of a cyber security degree. Thus, an application that is otherwise successful will remain as pending and an HEI will not be able to use or advertise its ACE-CSE recognition until Full certification is achieved. HEIs for which this applies will be given a maximum period of time in which to achieve Full Certification – it is anticipated that this will be six months.

There will be two levels of recognition:

- Gold Award for those applications that are meeting, or exceeding, all of the Gold Award requirements. An HEI with a successful application will be recognised as an 'Academic Centre of Excellence in Cyber Security Education – Gold Award'. The Gold Award will be awarded for a period of 5 years. Please see Appendix A for the required structure of an application for Gold Award.

[1] https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
[2] https://www.ncsc.gov.uk/section/education-skills/research-and-academia
[3] https://www.cybersecurity.ox.ac.uk/education/cdt
[4] https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/studying-here/centre-for-doctoral-training-in-cyber-security-for-the-everyday
[5] https://www.bristol.ac.uk/cdt/cyber-security/
[6] https://www.ucl.ac.uk/computer-science/study/postgraduate-research/cdt-cybersecurity
[7] https://www.ncsc.gov.uk/section/education-skills/higher-education

- Silver Award for those applications that meet all of the Silver Award requirements several of which require there to be convincing plans, fully supported by their HEI, to achieve the equivalent Gold Award requirements. An HEI with a successful application will be recognised as an 'Academic Centre of Excellence in Cyber Security Education – Silver Award'. The Silver Award will be awarded for a period of 3 years after which time an HEI will either have successfully gained Gold Award recognition or it will lose its ACE-CSE Silver Award recognition. Please note that a Silver Award will not be renewed. Please see Appendix B for the required structure of an application for Silver Award.

2 Background

2.1 Background to ACEs-CSR and ACEs-CSE

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. Currently, nineteen universities have been recognised as ACEs-CSR. Seven or so years on, government believes that the ACE-CSR programme has brought about considerable added value. For instance, it is clear that the programme has played an important role in establishing a community of cyber security researchers in the UK; it helped identify gaps in the research portfolio giving rise to Research Institutes being set up; and it has been the springboard for a number of other initiatives such as:

- NCSC-sponsored doctoral studentships across the ACEs-CSR (over 60 in number)
- NCSC small-grants programme
- Industrial sponsorship of cyber security research via the CyberInvest[8] programme

At the time of setting up the ACEs-CSR, it was government's intention to establish an equivalent for cyber security education. However, it soon became apparent that developing assessment criteria for ACEs-CSE would require more work and take some time to develop. The first step was to establish guidance for the cyber security content of degrees and develop an assessment framework that could be used for the certification of degrees. As a result, NCSC has established a programme for the certification of postgraduate Master's, Integrated Master's and Bachelor's degrees in cyber security. Currently, there are thirty-two certified degrees from twenty-one universities[9]. It is anticipated that these numbers will steadily grow.

[8] https://www.ncsc.gov.uk/information/cyber-invest
[9] https://www.ncsc.gov.uk/information/ncsc-certified-degrees

2.2 Complementary Initiatives

There are a number of complementary government activities that are of relevance to ACEs-CSE. For example:

- to help populate the cyber security pipeline, the CyberFirst[10] programme offers bursaries to undergraduate students, delivers short courses in cyber security for young people aged 11 – 19, and runs a Girls Competition
- led by DCMS, Cyber Discovery[11] is a programme of extra-curricular on-line activities and challenges for students aged 14 – 18 to introduce them to the field of cyber security
- the pilot, Gloucestershire-based, Cyber Schools Hub programme[12] aims to help students engage with computing and computational thinking as well as develop resources for teachers
- the National Centre for Computing[13] aims to support teachers in England with computer science teaching across the curriculum
- CISSE UK[14] is a collaboration between government, industry and the academic community to promote and establish outstanding cyber security education across the UK
- the Cyber Security Body of Knowledge (CyBOK) project[15] is identifying the foundational knowledge upon which the field of cyber security is based
- the Cyber Security Council project is putting in place a new overarching professional body for cyber security[16]
- DCMS and the Office for AI are funding postgraduate Master's conversion courses in AI and machine learning[17]

2.3 Proposition

Government believes that there is now a critical mass of universities with NCSC-certified cyber security degrees, and there are allied initiatives addressing the talent pipeline and cyber security/computing education in schools. Given these factors, government now considers it timely to initiate the ACE-CSE programme and would expect the ACEs-CSE to play an important role in helping to shape/support university and pre-university cyber security education across the UK.

3 Requirements for recognition as an ACE-CSE

Please note that ACE-CSE recognition will not be awarded until an HEI has full certification of at least one cyber security degree.

[10] https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds
[11] https://www.joincyberdiscovery.com
[12] https://www.ncsc.gov.uk/information/cyber-schools-hubs
[13] https://teachcomputing.org
[14] https://cisseuk.org/
[15] https://www.cybok.org
[16] https://eandt.theiet.org/content/articles/2019/08/iet-to-lead-creation-of-uk-cyber-security-council/
[17] https://www.officeforstudents.org.uk/advice-and-guidance/skills-and-employment/postgraduate-conversion-courses-in-data-science-and-artificial-intelligence/

3.1 Gold Award

Table 1 below shows the high-level requirements that must be met for an HEI to be recognised as an ACE-CSE – Gold Award. These should be read in conjunction with Appendix A which provides further detail of the requirements and how applications will be assessed against those requirements.

Requirement	Description
Gold Req 1	The senior management of the HEI must be committed to the consolidation and continued development of the proposed ACE-CSE.
Gold Req 2	The proposed ACE-CSE must be running at least one NCSC-certified cyber security degree with Full certification at undergraduate or postgraduate level.
Gold Req 3	The proposed ACE-CSE must be running a degree in computing at undergraduate or postgraduate level[18].
Gold Req 4	The proposed ACE-CSE must have a well-defined team comprising staff with expertise in cyber security and computing as well as staff: • responsible for communication and outreach • responsible for diversity and inclusion • from allied disciplines – by way of example, but not limited to, STEM, business, social science, etc. • with responsibilities for the computing and communications infrastructure at the HEI
Gold Req 5	The proposed ACE-CSE must present a coherent, ambitious and achievable strategy for consolidating and developing as an ACE-CSE.
Gold Req 6	The proposed ACE-CSE must be playing an important role in the teaching/raising awareness of cyber security, at an appropriate level, to students from across the HEI.
Gold Req 7	The proposed ACE-CSE must be supporting its senior management to tackle the cyber security of the HEI's computing and communication infrastructure.
Gold Req 8	The proposed ACE-CSE must demonstrate active and effective external engagement and outreach activities with, but not limited to, industry, local schools and colleges, under-represented communities, allied government initiatives, etc.

Table 1: *The high-level requirements an HEI must meet in order to achieve ACE-CSE recognition – Gold Award.*

3.2 Silver Award

Table 2 below shows the high-level requirements that must be met for an HEI to be recognised as an ACE-CSE – Silver Award. These should be read in conjunction with Appendix B which provides further detail of the requirements and how applications will be assessed against those requirements.

Requirement	Description
Silver Req 1	The senior management of the HEI must show strong support for the proposed ACE-CSE's plans under requirements Silver Req 4 to Silver Req 8.
Silver Req 2	The proposed ACE-CSE must be running at least one NCSC-certified cyber security degree with Full certification at undergraduate or postgraduate level.

[18] This requirement reflects government's view that a solid grounding in computing provides the foundations for cyber security education.

Silver Req 3	The proposed ACE-CSE must be running a degree in computing at undergraduate or postgraduate level[19].
Silver Req 4	The proposed ACE-CSE must have a well-defined team comprising staff with expertise in cyber security and computing. The team must be able to show that it has convincing and appropriate plans for extending the team to include staff: • responsible for communication and outreach • responsible for diversity and inclusion • from allied disciplines – by way of example, but not limited to, STEM, business, social science, etc. • with responsibilities for the computing and communications infrastructure at the HEI
Silver Req 5	The proposed ACE-CSE must present a coherent, ambitious and achievable strategy for developing as an ACE-CSE and achieving Gold Award recognition within three years of achieving Silver Award recognition.
Silver Req 6	**Either (Silver Req 6a)**: • The proposed ACE-CSE must present a coherent and appropriate plan for playing an important role in the teaching/raising awareness of cyber security, at an appropriate level, to students from across the HEI. **Or (Silver Req 6b)**: • **Gold Req 6**.
Silver Req 7	**Either (Silver Req 7a)**: • The proposed ACE-CSE must present a coherent and appropriate plan for supporting its senior management to tackle the cyber security of the HEI's computing and communication infrastructure. **Or (Silver Req 7b)**: • **Gold Req 7**.
Silver Req 8	**Either (Silver Req 8a)**: • The proposed ACE-CSE must present a coherent and appropriate plan for external engagement and outreach activities – with, but not limited to, industry, local schools and colleges, under-represented communities, allied government initiatives, etc. **Or (Silver Req 8b)**: • **Gold Req 8**.
Silver Req 9	This addresses the requirement that at least one of **Gold Req 6**, **Gold Req 7** or **Gold Req 8** must be achieved.

Table 2: *The high-level requirements an HEI must meet in order to achieve ACE-CSE recognition – Silver Award*

4 Aims and benefits of the ACE-CSE programme

The overall aim is to recognise those UK universities whose approach to cyber security education is excellent and who are engaging both across their universities as well as externally with the wider community. The anticipated key benefits include:

- establishing a community from across academia, government and industry concerned with developing, improving and bringing coherence to cyber security education both at degree and pre-university levels

[19] This requirement reflects government's view that a solid grounding in computing provides the foundations for cyber security education.

- helping ACEs-CSE to attract both internal and external funding to support their cyber security education activities
- helping ACEs-CSE to attract additional numbers / higher quality students both from the UK and the rest of the world
- helping employers (in industry, government and academia) during the recruitment process to better understand the cyber security education that applicants have received, both for cyber security and computing specialists as well as students from other disciplines
- by having NCSC-certified degrees in cyber security, helping ACEs-CSE to produce excellent graduates able to enter the cyber security workplace who are highly valued by industry, government and academia
- ACEs-CSE supporting efforts to improve the cyber resilience of their HEIs
- enabling ACEs-CSE to act as, and be recognised as, beacons of outreach activities in their areas helping to bring more people into the field

5 Funding

Whilst there is currently no funding available for those HEIs achieving ACE-CSE recognition, there may be plans to make funding available in the future.

It is anticipated that future calls for education-related activities which attract funding (e.g., running of cyber security courses for young people) may be directed towards ACEs-CSE.

6 Eligibility

This Call for applications is open to all UK HEIs that on the census date of Wednesday 1st April 2020 have at least one NCSC certified cyber security degree with Full or Provisional certification.

7 How to apply

7.1 Expressions of Interest

To help the NCSC plan for assessments, all HEIs intending to apply for ACE-CSE recognition must submit an Expression of Interest (EOI) by the deadline of Wednesday 22nd April 2020. The NCSC will confirm receipt of the EOI by email.

7.2 Submitting applications

Applications should be emailed to ace-cse@ncsc.gov.uk by 16:00 on Thursday 14th May 2020. 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, or connected with, 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).

7.3 Guidance on writing applications

Applicants should apply for Gold Award or Silver Award and should follow the guidance provided in Appendix A or Appendix B as appropriate.

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

7.4 Briefing sessions

Briefing sessions are planned on the afternoon of Wednesday 12th February 2020 in London and the afternoon of Wednesday 26th February 2020 in Manchester. Please email ace-cse@ncsc.gov.uk at least 48 hours before the specific briefing session to register attendance. To help with administration, please put 'ACE-CSE briefing day - <Name of your HEI>' in the subject line. Please include the names and contact details of those wishing to attend the briefing meeting – maximum of 3 per HEI – and which briefing session you wish to attend.

7.5 Points of clarification

This call document and a list of points of clarification regarding the application process will be maintained at: https://www.ncsc.gov.uk/information/ace-cse-recognition-call

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 Friday 1st May 2020 to discuss any questions or areas of concern they might have. Please contact the NCSC at ace-cse@ncsc.gov.uk

8 Assessment

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

8.1 Assessment Process

8.1.1 Gold Award

At the assessment panel each application will be assessed within the eight areas shown in Table 3, and further described in Appendix A, against the set of assessment criteria also shown in Appendix A.

Section of Application	Requirements Addressed	Scoring
1. Statement of support from the HEI	**Gold Req 1**	Pass/Fail

2. NCSC-certified degrees	**Gold Req 2**	Pass/Fail
3. Degrees in Computing	**Gold Req 3**	Pass/Fail
4. Description of the proposed ACE-CSE	**Gold Req 4**	0 to 4
5. Description of the proposed ACE-CSE's strategy	**Gold Req 5**	0 to 4
6. Description of the proposed ACE-CSE's role in cyber security education across the HEI	**Gold Req 6**	0 to 4
7. Description of the proposed ACE-CSE's supporting role in addressing the cyber security of the HEI	**Gold Req 7**	0 to 4
8. Description of the proposed ACE-CSE's external engagement and outreach activities	**Gold Req 8**	0 to 4

Table 3: *Sections of a Gold Award application and the relevant requirements addressed*

8.1.2 Silver Award

At the Assessment Panel each application will be assessed within the nine areas shown in Table 4, and further described in Appendix B, against the set of assessment criteria also shown in Appendix B:

Section of Application	Requirements Addressed	Scoring
1. Statement of support from the HEI	**Silver Req 1**	Pass/Fail
2. NCSC-certified degrees	**Silver Req 2**	Pass/Fail
3. Degrees in computing	**Silver Req 3**	Pass/Fail
4. Description of the proposed ACE-CSE	**Silver Req 4**	0 to 4
5. Description of the proposed ACE-CSE's strategy	**Silver Req 5**	0 to 4
6. Description of the proposed ACE-CSE's role in cyber security education across the HEI	**Silver Req 6**	0 to 4
7. Description of the proposed ACE-CSE's supporting role in addressing the cyber security of the HEI	**Silver Req 7**	0 to 4
8. Description of the proposed ACE-CSE's external engagement and outreach activities	**Silver Req 8**	0 to 4
	Silver Req 9	Pass/Fail

Table 4: *Sections of a Silver Award application and the relevant requirements addressed*

8.2 Scoring

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 section of each application. In terms of providing evidence to meet the assessment criteria, each scored section of each application will be marked using the following scales:

Score	Meaning
0	No response or no response capable of assessment has been submitted, or the response does not address the criteria of the requirement.
1	The response meets some but not a majority of the requirement and/or insufficient evidence is provided to substantiate the response. There are significant deficiencies in the response.
2	The response meets the majority but not all of the requirement and there are minor deficiencies in how the application addresses the remaining criteria. For those parts of the requirement that are met, sufficient evidence to substantiate the response is provided.
3 (pass mark)	The response meets the requirement in full and is supported by evidence that substantiates the response. All of the criteria of the requirement are satisfactorily covered by the response.
4	The response meets, and in some places exceeds, the requirement. The response is backed up by substantial and convincing evidence.

Table 5: *Numeric scoring scale used to assess applications*

Score	Meaning
Fail	No response or no response capable of assessment has been submitted, or the response does not address the criteria of the requirement.
Pass	The requirement is met by the response.

Table 6: *Pass/Fail scoring scale used to assess applications*

The Panel's decision is final. There is no maximum number of successful applications for ACE-CSE recognition.

8.2.1 Gold Award

A successful application requires that each scored section must achieve a Pass or achieve a threshold score of 3.

8.2.2 Silver Award

A successful application requires that each scored section must achieve a Pass or achieve a threshold score of 3. In addition, **Silver Req 9** must achieve a Pass.

9 Moving forwards

9.1 Key dates

Activity	Proposed Date
Call issued	Week beginning 20th January 2020
Deadline for briefing sessions registration	48 hours before each briefing session
Briefing session London	Wednesday 12th February 2020
Briefing session Manchester	Wednesday 26th February 2020
Deadline for Expressions of Interest	Wednesday 22nd April 2020
Deadline for submission of applications	Thursday 14th May 2020, 1600
Assessment of proposals	May to July 2020
Announcement of results	Late July 2020

9.2 Future calls

It is anticipated that future calls for ACEs-CSE will be issued in 2021 and 2022.

9.3 After the assessment process

All applicants will be notified individually whether their applications have been successful, and arrangements will be made for a formal announcement.

9.4 Successful applications

9.4.1 Gold Award

An HEI will be recognised as an 'Academic Centre of Excellence in Cyber Security Education – Gold Award' for a period of five years, subject to the HEI agreeing the T&Cs that will document the ongoing requirements for both the ACE-CSE and government. One such requirement will be for an ACE-CSE to have at least one NCSC certified degree with full certification throughout the period of ACE-CSE recognition. After the five-year period, it is anticipated that an HEI will need to submit a new application in order to renew its ACE-CSE Gold Award recognition.

9.4.2 Silver Award

An HEI will be recognised as an 'Academic Centre of Excellence in Cyber Security Education – Silver Award' for a period of three years, subject to the HEI agreeing the T&Cs that will document the ongoing requirements for both the ACE-CSE and government. One such requirement will be for an ACE-CSE to have at least one NCSC certified degree with full certification throughout the period of ACE-CSE recognition. After the three-year period, an HEI will not be able to re-apply for ACE-CSE Silver Award but must, if it wishes to retain ACE-CSE recognition, apply for the Gold Award.

9.5 Unsuccessful applications

Applications that are not successful in this call will be given written feedback and offered a face-to-face feedback session.

9.5.1 Unsuccessful Gold Award applications

If the assessment panel finds that an unsuccessful Gold Award application from an HEI that has not previously held a Silver Award meets, or could meet with minor updates, the criteria for Silver

Award, then at the panel's discretion the panel may choose to recognise the HEI as an ACE-CSE with Silver Award.

Appendix A: Required structure of applications for ACE-CSE recognition – Gold Award

This appendix provides details of the information that applicants should provide with their application along with the criteria that will be applied. All information provided will be treated confidentially and not shared by government except for the purposes of the assessment process – though please see paragraphs immediately below.

It is expected that applications received in response to this call will contain much valuable insight and information on current UK academic cyber security education 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 education policies and strategies.

In your covering email please indicate whether you are happy for the information in your application to be used for this additional purpose. The ACE-CSE 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 academics to be identified.

Please note that an HEI must only submit one application against this call and the lead department making the application must hold an NCSC-certified undergraduate or postgraduate degree in cyber security (Provisional or Full).

Documents should be in pdf format, no larger than 15MB, with the font size no smaller than 10pt. Unless specifically asked for, additional pages and other material in addition to that outlined below will not be read and will not therefore form part of the assessment for certification.

Applications must be well signposted, using bookmarks, page numbers, headers and footers. They should contain a contents page and should follow the structure of the Call document using sub-headings.

Each application should comprise the following eight sections:

1. ‘Statement of support from the HEI’ (**up to two sides of A4**).
2. ‘NCSC-certified degrees’ (**up to one side of A4**).
3. ‘Degrees in computing’ (**up to two sides of A4**)
4. ‘Description of the proposed ACE-CSE’ (**up to five sides of A4, excluding CVs**).
5. ‘Description of the proposed ACE-CSE’s strategy’ (**up to five sides of A4**).
6. ‘Description of the proposed ACE-CSE’s role in cyber security education across the HEI’ (**up to five sides of A4**).
7. ‘Description of the proposed ACE-CSE’s role in addressing the cyber security of the HEI’ (**up to five sides of A4**).
8. ‘Description of the proposed ACE-CSE’s external engagement and outreach activities’ (**up to five sides of A4**)

1 Statement of support from the HEI (up to two sides of A4)

Please provide a signed statement of support from the Vice Chancellor (or equivalent) supporting the HEI's application for ACE-CSE recognition – Gold Award and that demonstrates the HEI's continued commitment to:

- cyber security in the HEI's future strategy
- investment in the area of the proposed ACE-CSE
- cyber security education in the department(s) which have a certified degree as well as across the student body of the HEI as a whole
- working with the proposed ACE-CSE to help improve the cyber security awareness of the HEI's workforce
- working with the proposed ACE-CSE to help address the cyber security of the HEI's computing and communications infrastructure
- supporting the proposed ACE-CSE's external engagement activities

1.1 Assessment criteria – scored as Pass or Fail

These criteria address **Gold Req 1**.

The HEI's senior management must support the application and demonstrate the commitment required to consolidate, and continue the development of, the proposed ACE-CSE.

2 NCSC-certified degrees (up to one side of A4)

Please provide a table of the proposed ACE-CSE's cyber security degrees that have achieved NCSC certification. For each certified degree, please include the following information:

- the name of the degree
- the degree awarded, e.g, BSc, MComp, MSc, etc.
- Provisional or Full certification
- the certification start and end dates
- whether the degree is running in academic year 2019 – 2020.

2.1 Assessment criteria – scored as Pass or Fail

These criteria address **Gold Req 2**.

The proposed ACE-CSE must be running at least one NCSC-certified cyber security degree with Full certification at undergraduate or postgraduate level.

3 Degrees in computing (up to two sides of A4)

Please provide a table of the degrees in computing being run by the proposed ACE-CSE. For each degree, please include the following information:

- the name of the degree
- the degree awarded, e.g, BSc, MComp, MSc, etc.
- whether the degree is running in academic year 2019 – 2020.

3.1 Assessment criteria – scored as Pass or Fail

These criteria address **Gold Req 3**.

The proposed ACE-CSE must be running a degree in computing at undergraduate or postgraduate level.

4 Description of the proposed ACE-CSE (up to five sides of A4, excluding CVs)

Please provide the following information:

a. Please describe the team that will run the ACE-CSE. This should include, for example, the ACE-CSE Director, the key team members, roles and responsibilities, and the lead department(s) involved.
b. Please describe how the team has the necessary cyber security expertise to engage both within its university and externally.
c. Please provide a CV (two sides of A4 maximum) for each key team member of staff that highlights their role and relevant expertise in the ACE-CSE. The CVs should be placed in an appendix to section 4.

4.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Gold Req 4**.

i. There must be a clearly identified coherent team responsible for running the proposed ACE-CSE.
ii. Team members of the proposed ACE-CSE must have clearly defined roles and responsibilities along with the appropriate expertise.
iii. The application must demonstrate that the team has the critical mass to undertake its activities, deliver its strategy and include:
    - staff with expertise in cyber security and computing
    - staff responsible for communication and outreach
    - staff responsible for diversity and inclusion
    - staff from allied disciplines – by way of example, but not limited to, STEM, business, social science, etc.
    - staff with responsibilities for the computing and communications infrastructure at the HEI

5 Description of the proposed ACE-CSE's strategy (up to five sides of A4)

Please describe the proposed ACE-CSE's strategy for consolidation and development over the next five-year period. By way of example, this might include plans for:

- growth in staff numbers and expertise
- introducing new cyber security and computing degrees, including degree apprenticeships

- exploring different teaching and learning styles as well as different modes of presentation (full-time, part-time, distance learning, block release, etc.)
- further investment in facilities
- further promotion of cyber security across the HEI
- deepening the engagement with industry as well as government and other academic institutions
- influencing and keeping at the forefront of cyber security education by, for example, actively participating in national and international fora

5.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Gold Req 5**.

i. The proposed ACE-CSE must present a clear, coherent, ambitious and achievable strategy for consolidation and development over the next five years.
ii. The proposed ACE-CSE must demonstrate its intentions to continue to engage effectively internally within its HEI.
iii. The proposed ACE-CSE must demonstrate its intention to continue, and further strengthen, its engagement with partners in industry as well as other academic institutions and government.
iv. The proposed ACE-CSE must demonstrate its intention to continue, and further strengthen, its work on cyber security education issues at national/international levels.

6 Description of the proposed ACE-CSE's role in cyber security education across the HEI (up to five sides of A4)

Explanatory note: it would not be expected that an ACE-CSE could instigate such activities by itself. It requires the senior management of the HEI to drive, and set the goals for, such activities and for an ACE-CSE to advise and support. This is why HEI buy-in for an ACE-CSE is so important.

Please describe how the proposed ACE-CSE supports cyber security education across the HEI. For example, this might cover:

a. The role that the proposed ACE-CSE plays in supporting and implementing cyber security education across the HEI.
b. For computer science undergraduate students who are not specialising in cyber security:
    - the introduction of cyber security module(s); and/or
    - the introduction of the Information Assurance and Security Knowledge Area from the ACM/IEEE Computer Science curriculum into undergraduate computer science degrees[20]; and/or
    - the introduction of appropriate Knowledge Areas from the Cyber Security Body of Knowledge[21]

[20] https://www.acm.org/education/curricula-recommendations
[21] https://www.cybok.org/

c. Working with the HEI's departments outside of computing and cyber security to help ensure these departments make their students aware of at least the basics of good cyber security practice – for example:
    - introduction of a 'cyber security 101' module for students
    - providing lectures or guides to working securely in the digital world
    - running cyber security challenges for departments outside of computing and cyber security

6.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Gold Req 6**.

i. It must be clear that the proposed ACE-CSE is playing an important role in cyber security education across the HEI.
ii. Undergraduate computer science students who are not specialising in cyber security are covering the foundations of cyber security.
iii. Students outside of computing and cyber security are being introduced to the importance of good cyber security.

7 Description of the proposed ACE-CSE's supporting role in addressing the cyber security of the HEI (up to five sides of A4)

Explanatory note: a cyber security strategy for an HEI will be developed and driven by the senior management of the HEI and the IT department (or equivalent). It would, therefore, not be expected that an ACE-CSE would instigate HEI-wide cyber security activities. The ACE-CSE could, however, advise and support the cyber security strategy for the HEI.

Please describe how the proposed ACE-CSE supports cyber security across the HEI. For example, this might include:

a. The role that the proposed ACE-CSE plays in supporting and implementing cyber security for the HEI.
b. The role that the proposed ACE-CSE plays in supporting the HEI's senior management with, for example:
    - senior-level awareness of cyber security
    - cyber security policies and practices across the HEI
    - supporting HEI cyber security training and awareness raising of both staff and students
    - supporting the HEI to maintain and improve the cyber security of the HEI's computing and communications infrastructure, which could include the achievement of Cyber Essentials Certification[22] or other recognised industry standards

[22] https://www.cyberessentials.ncsc.gov.uk/

7.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Gold Req 7**.

i. It must be clear that the proposed ACE-CSE plays an important role in the cyber security of the HEI.
ii. The proposed ACE-CSE must be supporting and engaging with its senior management to tackle the workforce's awareness of the need for good cyber security.
iii. The proposed ACE-CSE must be supporting and engaging with its senior management to tackle the cyber security of the HEI's computing and communication infrastructure.

8 Description of the proposed ACE-CSE's external engagement and outreach activities (up to five sides of A4)

Explanatory note: the context for this requirement is the ambition set out in the UK's National Cyber Security Strategy[23] for the UK to "have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors." For example, outreach activities could clearly play an important role in engaging with young people – both in educating them about the need for good cyber security and encouraging them to think about a future career in the field. In addition, outreach activities may also be expected to support school teachers with lesson plans and teaching materials, as well as people in mid-career or returners to work looking to enter the cyber security job market.

Please describe the proposed ACE-CSE's external engagement to date and future plans. For example, this might cover:

a. external engagement activities with industry, government and academia in cyber security, key outcomes to date, and how these add value to the ACE-CSE and its cyber security education programme
b. outreach activities with the wider community and key outcomes to date, for example:
   - with schools, teacher organisations, under-represented groups, community groups and the like
   - covering cyber security as well as basic cyber awareness
   - providing support to school teachers with the teaching of cyber security and cyber awareness
c. the problems to be addressed in future work in this area together with the outcomes that the HEI hopes to achieve

8.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Gold Req 8**.

i. It must be clear that the proposed ACE-CSE has a good range of external linkages that add value to its cyber security education programme.
ii. It must be clear that the proposed ACE-CSE engages effectively with the wider community.

[23] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

iii. It must be clear that the proposed ACE-CSE has demonstrated clear outreach achievements and impacts to date and has a coherent and viable future strategy that addresses important outreach issues.

Appendix B: Required structure of applications for ACE-CSE recognition – Silver Award

This appendix provides details of the information that applicants should provide with their application along with the criteria that will be applied. All information provided will be treated confidentially and not shared by government except for the purposes of the assessment process – though please see paragraphs immediately below.

It is expected that applications received in response to this call will contain much valuable insight and information on current UK academic cyber security education 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 education policies and strategies.

In your covering email please indicate whether you are happy for the information in your application to be used for this additional purpose. The ACE-CSE 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 academics to be identified

Please note that an HEI must only submit one application against this Call and the lead department making the application must hold an NCSC-certified undergraduate or postgraduate degree in cyber security with Full certification.

Documents should be in pdf format, no larger than 15MB, with the font size no smaller than 10pt. Unless specifically asked for, additional pages and other material in addition to that outlined below will not be read and will not therefore form part of the assessment for certification.

Applications must be well signposted, using bookmarks, page numbers, headers and footers. They should contain a contents page and should follow the structure of the Call document using sub-headings.

Each application should comprise the following eight sections:

1. 'Statement of support from the HEI' (**up to two sides of A4**).
2. 'NCSC-certified degrees' (**up to one side of A4**).
3. 'Degrees in computing' (**up to two sides of A4**)
4. 'Description of the proposed ACE-CSE' (**up to five sides of A4, excluding CVs**).
5. 'Description of the proposed ACE-CSE's strategy' (**up to five sides of A4**).
6. 'Description of the proposed ACE-CSE's role in cyber security education across the HEI' (**up to five sides of A4**).
7. 'Description of the proposed ACE-CSE's supporting role in addressing the cyber security of the HEI' (**up to five sides of A4**).
8. 'Description of the proposed ACE-CSE's external engagement and outreach activities' (**up to five sides of A4**)

1 Statement of Support from the HEI (up to two sides of A4)

Please provide a signed statement of support from the Vice Chancellor (or equivalent) supporting the HEI's application for ACE-CSE recognition – Silver Award and that demonstrates full support for the proposed ACE-CSE in its:

- plan to augment the team with staff responsible for, for example:
  - communication and outreach
  - diversity and inclusion
  - allied disciplines
  - computing and communications infrastructure at the HEI
- plan for development over the next three years
- proposed role for cyber security education across the HEI
- proposed supporting role for the cyber security of the HEI
- plan for external engagement and outreach

1.1 Assessment criteria – scored as Pass or Fail

These criteria address **Silver Req 1**.

The HEI's senior management must support the application and show strong support for the proposed ACE-CSE's plans under requirements Silver Req 4 to Silver Req 8.

2 NCSC-certified degrees (up to one side of A4)

Please provide a table of the proposed ACE-CSE's cyber security degrees that have achieved NCSC certification. For each certified degree, please include the following information:

- the name of the degree
- the degree awarded, e.g, BSc, MComp, MSc, etc.
- Provisional or Full certification
- the certification start and end dates
- whether the degree is running in academic year 2019 – 2020.

2.1 Assessment criteria – scored as Pass or Fail

These criteria address **Silver Req 2**.

The proposed ACE-CSE must be running at least one NCSC-certified cyber security degree with Full certification at undergraduate or postgraduate level.

3 Degrees in computing (up to two sides of A4)

Please provide a table of the degrees in computing being run by the proposed ACE-CSE. For each degree, please include the following information:

- the name of the degree
- the degree awarded, e.g, BSc, MComp, MSc, etc.
- whether the degree is running in academic year 2019 – 2020.

3.1 Assessment criteria – scored as Pass or Fail

These criteria address **Silver Req 3**.

The proposed ACE-CSE must be running a degree in computing at undergraduate or postgraduate level.

4 Description of the proposed ACE-CSE (up to five sides of A4, excluding CVs)

Please provide the following information:

a. Please describe the team that will run the ACE-CSE. This should include, for example, the ACE-CSE Director, the key members of staff, roles and responsibilities, and the lead department(s) involved.
b. Please describe how the team has the necessary cyber security expertise to engage both within its university and externally.
c. Please describe plans to augment the team with staff responsible for, for example:
    - communication and outreach
    - diversity and inclusion
    - allied disciplines (by way of example, but not limited to, STEM, business, social science, etc.)
    - computing and communications infrastructure at the HEI
d. Please provide a CV (two sides of A4 maximum) for each key member of staff that highlights their role and relevant expertise in the ACE-CSE. The CVs should be placed in an appendix to section 4.

4.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 4**.

i. There must be a clearly identified coherent team responsible for running the proposed ACE-CSE.
ii. Team members of the proposed ACE-CSE must have clearly defined roles and responsibilities along with the appropriate expertise.
iii. There must be a coherent and appropriate plan to augment the team.

5 Description of the proposed ACE-CSE's strategy (up to five sides of A4)

Please describe the proposed ACE-CSE's strategy for development and achieving Gold Award recognition within three years of achieving Silver Award recognition. By way of example, this might include plans for:

- growth in staff numbers and expertise
- introducing new cyber security and computing degrees, including degree apprenticeships
- exploring different teaching and learning styles as well as different modes of presentation (full-time, part-time, distance learning, block release, etc.)

- investment in facilities
- promoting cyber security across the HEI
- engagement with industry as well as government and other academic institutions
- influencing and keeping at the forefront of cyber security education by, for example, actively participating in national and international fora

5.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 5**.

i. The proposed ACE-CSE must present a clear, coherent, ambitious and achievable strategy for development and achieving Gold Award recognition within three years of achieving Silver Award recognition.
ii. The proposed ACE-CSE must demonstrate its intentions to engage effectively internally within its HEI.
iii. The proposed ACE-CSE must demonstrate its intentions to engage effectively externally with partners in industry as well as other academic institutions and government.
iv. The proposed ACE-CSE must demonstrate its intention to engage with cyber security education issues at national/international levels.

6 Description of the proposed ACE-CSE's role in cyber security education across the HEI (up to five sides of A4)

Explanatory note: it would not be expected that the ACE-CSE could instigate such activities by itself. It requires the senior management of the HEI to drive, and set the goals for, such activities and for the ACE-CSE to advise and support. This is why HEI buy-in for the ACE-CSE is so important.

*Applicants should complete section 6.1 (**Silver Req 6a**) or 6.2 (**Silver Req 6b**)*

6.1 Silver Req 6a

Please describe the proposed ACE-CSE's plans to support cyber security education across the HEI. For example, this might cover:

a. The role that the proposed ACE-CSE could play in supporting and implementing cyber security education across the HEI.
b. For computer science undergraduate students who are not specialising in cyber security:
    - the introduction of cyber security module(s); and/or
    - the introduction of the Information Assurance and Security Knowledge Area from the ACM/IEEE Computer Science curriculum into undergraduate computer science degrees[24]; and/or
    - the introduction of appropriate Knowledge Areas from the Cyber Security Body of Knowledge[25]

[24] https://www.acm.org/education/curricula-recommendations
[25] https://www.cybok.org/

c. Working with the HEI's departments outside of computing and cyber security to help ensure these departments make their students aware of at least the basics of good cyber security practice – for example:
    - introduction of a 'cyber security 101' module for students
    - providing lectures or guides to working securely in the digital world
    - running cyber security challenges for departments outside of computing and cyber security

6.1.1 Assessment criteria – scored on scale of 0 to 4

These criteria address Silver **Req 6a**.

i. It should be clear that the proposed ACE-CSE would be expected to play an important role in cyber security education across the HEI.
ii. There are plans to ensure that undergraduate computer science students who are not specialising in cyber security should cover the foundations of cyber security.
iii. There are plans to ensure that students outside of computing and cyber security are also being introduced to the importance of good cyber security.

6.2 Silver Req 6b (equivalent to Gold Req 6)

Please describe how the proposed ACE-CSE supports cyber security education across the HEI. For example, this might cover:

a. The role that the proposed ACE-CSE plays in supporting and implementing cyber security education across the HEI.
b. For computer science undergraduate students who are not specialising in cyber security:
    - the introduction of cyber security module(s); and/or
    - the introduction of the Information Assurance and Security Knowledge Area from the ACM/IEEE Computer Science curriculum into undergraduate computer science degrees[26]; and/or
    - the introduction of appropriate Knowledge Areas from the Cyber Security Body of Knowledge[27]
c. Working with the HEI's departments outside of computing and cyber security to help ensure these departments make their students aware of the basics of good cyber security practice – for example:
    - introduction of a 'cyber security 101' module for students
    - providing lectures or guides to working securely in the digital world
    - running cyber security challenges for departments outside of computing and cyber security

6.2.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 6b (equivalent to Gold Req 6)**.

[26] https://www.acm.org/education/curricula-recommendations
[27] https://www.cybok.org/

i. It must be clear that the proposed ACE-CSE is playing an important role in cyber security education across the HEI.
ii. Undergraduate computer science students who are not specialising in cyber security are covering the foundations of cyber security.
iii. Students outside of computing and cyber security are being introduced to the importance of good cyber security.

7 Description of the proposed ACE-CSE's supporting role in addressing the cyber security of the HEI (up to five sides of A4)

Explanatory note: a cyber security strategy for the HEI will be developed and driven by the senior management of the HEI and the IT department (or equivalent). It would, therefore, not be expected that the ACE-CSE would instigate HEI-wide cyber security activities. The ACE-CSE could, however, advise and support the cyber security strategy for the HEI.

*Applicants should complete section 7.1 (**Silver Req 7a**) or 7.2 (**Silver Req 7b**)*

7.1 Silver Req 7a

Please describe the proposed ACE-CSE's plans to support cyber security across the HEI. For example, this might include:

a. The role that the proposed ACE-CSE could play in supporting and implementing cyber security for the HEI.
c. The role that the proposed ACE-CSE could play in supporting the HEI's senior management with, for example:
    - senior-level awareness of cyber security
    - cyber security policies and practices across the HEI
    - supporting HEI cyber security training and awareness raising of both staff and students
    - supporting the HEI to maintain and improve the cyber security of the HEI's computing and communications infrastructure, which could include achieving Cyber Essentials Certification[28] or other recognised industry standards

7.1.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 7a**.

i. It must be clear that the proposed ACE-CSE would be expected to play an important role in the cyber security of the HEI.
ii. The proposed ACE-CSE must present a convincing plan for engagement with its senior management to tackle the workforce's awareness of the need for good cyber security.
iii. The proposed ACE-CSE must present a convincing plan for engagement with its senior management to tackle the cyber security of the HEI's computing and communication infrastructure.

[28] https://www.cyberessentials.ncsc.gov.uk/

7.2 Silver Req 7b (equivalent to Gold Req 7)

Please describe how the proposed ACE-CSE supports cyber security across the HEI. For example, this might include:

a. The role that the proposed ACE-CSE plays in supporting and implementing cyber security for the HEI.
b. The role that the proposed ACE-CSE plays in supporting the HEI's senior management with, for example:
    - senior-level awareness of cyber security
    - cyber security policies and practices across the HEI
    - supporting HEI cyber security training and awareness raising of both staff and students
    - supporting the HEI to maintain and improve the cyber security of the HEI's computing and communications infrastructure, which could include the achievement of Cyber Essentials Certification[29] or other recognised industry standards

7.2.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 7b (equivalent to Gold Req 7)**.

i. It must be clear that the proposed ACE-CSE plays an important role in the cyber security of the HEI.
ii. The proposed ACE-CSE must be supporting and engaging with its senior management to tackle the workforce's awareness of the need for good cyber security.
iii. The proposed ACE-CSE must be supporting and engaging with its senior management to tackle the cyber security of the HEI's computing and communication infrastructure.

8 Description of the proposed ACE-CSE's external engagement and outreach activities (up to five sides of A4)

Explanatory note: the context for this requirement is the ambition set out in the UK's National Cyber Security Strategy[30] for the UK to "have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors." For example, outreach activities could clearly play an important role in engaging with young people – both in educating them about the need for good cyber security and encouraging them to think about a future career in the field. In addition, outreach activities may also be expected to support school teachers with lesson plans and teaching materials, as well as people in mid-career or returners to work looking to enter the cyber security job market.

*Applicants should complete section 8.1 (**Silver Req 8a**) **or** 8.2 (**Silver Req 8b**)*

[29] https://www.cyberessentials.ncsc.gov.uk/
[30] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

8.1 Silver Req 8a

Please describe the proposed ACE-CSE's current and future plans for external engagement. For example, this might cover:

a. current and future plans the ACE-CSE has for external engagement activities with industry, government and academia in cyber security and how these would be expected to add value to the ACE-CSE and its cyber security education programme
b. current and future plans for outreach activities in cyber security that the proposed ACE-CSE has with the wider community, for example
   - with schools, teacher organisations, under-represented groups, community groups and the like
   - covering cyber security as well as basic cyber awareness
   - providing support to schoolteachers with the teaching of cyber security and cyber awareness

8.1.1 Assessment criteria – scored on scale of 0 to 4

These criteria address **Silver Req 8a**.

i. It must be clear that the proposed ACE-CSE has, and proposes to further develop, a good range of external linkages that add value to its cyber security education programme.
ii. It must be clear that the proposed ACE-CSE engages with the wider community and has clear ideas on how this could be very effectively enhanced and further developed.

8.2 Silver Req 8b (equivalent to Gold Req 8)

Please describe the proposed ACE-CSE's external engagement to date and future plans. For example, this might cover:

a. external engagement activities with industry, government and academia in cyber security, key outcomes to date, and how these add value to the ACE-CSE and its cyber security education programme
b. outreach activities with the wider community and key outcomes to date, for example
   - with schools, teacher organisations, under-represented groups, community groups and the like
   - covering cyber security as well as basic cyber awareness
   - providing support to school teachers with the teaching of cyber security and cyber awareness
c. the problems to be addressed in future work in this area together with the outcomes that the HEI hopes to achieve

8.2.1 Assessment criteria – scored on scale of 0 to 4

These criteria address requirement **Silver Req 8b** (**equivalent to Gold Req 8)**

i. It must be clear that the proposed ACE-CSE has a good range of external linkages that add value to its cyber security education programme.
ii. It must be clear that the proposed ACE-CSE engages effectively with the wider community.

iii. It must be clear that the proposed ACE-CSE has demonstrated clear outreach achievements and impacts to date and has a coherent and viable future strategy that addresses important outreach issues.