DCMS

Embedding standards and pathways across the cyber profession by 2025

Submission from the Chartered Institution of Building Services Engineers (CIBSE)

19th March 2022

Name:	Dr Hywel Davies
Position:	Technical Director
Name of organisation:	Chartered Institution of Building Services Engineers
Address:	222 Balham High Road, London, SW12 9BS
Email address:	hdavies@cibse.org

About the Chartered Institution of Building Services Engineers (CIBSE)

The Chartered Institution of Building Services Engineers, CIBSE, is the professional engineering institution that exists to 'support the Science, Art and Practice of building services engineering, by providing our members and the public with first class information'. With its main office in London, CIBSE has over 20,000 members, with around 75% operating in the UK and many of the remainder in the Gulf, Hong Kong and Australasia. CIBSE accredits building services engineering courses in the UK and overseas.

CIBSE is the sixth largest professional engineering Institution, and along with the Institution of Structural Engineers is the largest dedicated to engineering in the built environment. Our members have international experience and knowledge of life safety requirements in many other jurisdictions and work extensively on the systems that control the various engineering systems that keep buildings safe, comfortable and healthy.

CIBSE members design, install, operate, maintain and refurbish life safety and energy using systems installed in buildings. They include specialists in digital engineering, the Society of Digital Engineering, a Division of CIBSE, who specialise in digital information management. We also have a Special Interest Group in IT and Building Controls, which works closely with the Building Controls Industry Alliance (BCIA) to provide events and activities on this topic.

CIBSE publishes Guidance and Codes providing best practice advice and internationally recognised as authoritative. These include the Digital Engineering Series of guidance and templates has been produced to assist the full built environment supply chain in tackling the practical challenges, specifically of the BIM processes, of digital engineering more widely.

The CIBSE Knowledge Portal makes our Guidance available online, where CIBSE members can access the guidance as a benefit of membership. The knowledge portal is the leading systematic engineering resource for the building services sector, used regularly by members to access the latest guidance material for the profession. Currently we have users in over 170 countries, demonstrating the world leading position of UK engineering expertise in this field.

CONSULTATION RESPONSE

Executive summary

This is the Institution's formal response to the consultation[1] issued by the Department of Digital, Media, Culture and Sport on "embedding standards and pathways across the cyber profession by 2025." As well as responding to the specific questions raised in the consultation, it also highlights other related considerations around professional recognition and regulation, in particular in relation to building safety.

CIBSE welcomes the government's proposals to regulate those who provide cybersecurity services, noting the very serious life safety, business integrity and national security implications of their work. Within the built environment that are many aspects of engineering systems within buildings that require cybersecurity expertise. Many of the systems that heat, cool, ventilate, illuminate buildings have software based control systems. Lifts and life safety systems are installed in many buildings and have software based control systems. All of these require consideration of cybersecurity. It is essential that building related systems are kept separate from business systems operating within the building. All of these require cybersecurity considerations to be taken into account.

There is also growing use of digital systems for the management of building related information during the design, construction and operation of buildings. This includesi the new digital "Golden Thread" of building information that will be required under the Building Safety Bill. This will also require cybersecurity measures and so will be regulated.

However, there is a significant unintended consequence arising from the proposal to regulate cybersecurity. It creates a potential scenario in which those who are responsible for the cybersecurity aspects of a building are regulated, whilst those responsible for other life safety aspects of the building engineering, such as structural, fire or building services aspects, continue to operate in an unregulated environment. To put it very starkly, the engineer who designs the structure of a skyscraper will be unregulated, whilst the engineer responsible for the cybersecurity of the information model that includes that structural design will be regulated. We believe that this is an entirely unintended outcome and also an entirely undesirable outcome that will be very hard to justify to residents in high rise buildings or indeed the wider public.

It is not just in the built environment where there may be a need for a wider consideration of regulation. As the UK seeks to make its way as Global Britain it seeks to be a leader in innovation and growth, often in high tech and IT related products and systems. To achieve a sustainable growth pathway in these fields will certainly require high professional standards. However, these will need to cover not just cybersecurity but other specialisms including data science, artificial intelligence, software engineering and health informatics. Whilst health informatics falls outside the built environment, there are already ideas about the use of

[1] https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025

articicial intelligence and data science to improve the management of buildings, ideas which may well create ethical challenges and will require professional responsibility to take forward.

CIBSE therefore recommends that standards of professionalism in a wider range of strategically significant information technology and management specialisms should also be supported and recognised by government alongside the very welcome and important attention to cyber security.

There is already an established structure of professional engineering recognition through the Engineering Council and CIBSE welcomes the opportunity to contribute to the development of appropriate professional recognition for cyber security and information management professionals. There may also be opportunities to work on contextualising existing engineering recognition and CIBSE would welcome the opportunty to discuss these with the Department and with the UK Cyber Security Council and to work with them to deliver enhanced standards of professional practice in cybersecurity in the built environment.

Consultation questions

Question 1. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that the market is best placed to define and embed professional standards?

Mostly disagree – if higher standards were a market solution this consultation would not be needed.

Question 2. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that government intervention is required to support this approach?

Mostly agree for the reason given in response to Q1.

Question 3. To what extent do you agree or disagree, ranging from fully agree to fully disagree, with the proposal that the UK Cyber Security Council should be formally recognised (via legislation) as the standard setting body for the cyber profession with a view to it overseeing the regulation of the profession under a legislative scheme?

Neither agree nor disagree.

Question 3a. Please expand on the reasons for this response?

The key outcome is for the regulation of cybersecurity professionals to be fully integrated with the regulation of other information professionals and other related professions in a coherent and effective overall system of professional regulation.

Question 4. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that regulating by activity should be explored in future plans?

Mostly agree

Question 5. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that under-qualified professionals should be prohibited from carrying out activities related to a specialism until they are qualified to do so?

Neither agree nor disagree. For some sensitive roles it may be appropriate, for other roles it may not. There will be a period during which formal qualification, or recognition of competence is being obtained by existing practitioners which will require a careful management of the transition to a regulated profession.

Question 6. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that role definitions across cyber security functions are inconsistently defined and require consolidation?

Fully disagree

Question 7. Do you think there are any additional considerations that need to be examined to ensure that the proposed measures to regulate professional job titles do not provide unnecessary barriers to entry for candidates entering or wishing to progress in a cyber security career?

Yes
Question 7a. What additional measures should be considered? [Open-ended question]

The proposals will need further development. In the built environment the interaction with other professional disciplines will need to be addressed.

Question 8. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that the profession should regulate the use of professional job titles?

There is a much wider question about regulation of professional job titles and this specific role needs to be addressed in that context.

Question 9. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that individuals should have to meet particular competency standards set by the UK Cyber Security Council in order to utilise a specific job title?

There is a much wider question about regulation of professional job titles and this question needs to be addressed in that context.

Question 10. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that statutory regulation on the use of title will not significantly exacerbate the existing skills shortage across cyber security roles in the UK?

Fully disagree

Questions 11-20: CIBSE is not an employer and so we have not answered these questions.

Question 11. As an employer, to what extent do you agree or disagree, ranging from fully agree to fully disagree, that you would prioritise recruitment of professionals with a job title recognised by the UK Cyber Security Council?

Question 12: As an employer, to what extent do you agree or disagree, ranging from fully agree to fully disagree, that your recruitment practice would be improved by having a clear, competence framework underpinned by legislation for cyber professionals to adhere to?

Question 13. As an employer, to what extent do you agree or disagree, ranging from fully agree to fully disagree, that you would support staff with their continuous professional development to achieve a job title recognised by the UK Cyber Security Council?

Question 14. As an employee, would you apply to obtain qualifications towards a professional job title recognised by the UK Cyber Security Council?

Question 15. As an employee, to what extent do you agree or disagree, ranging from fully agree to fully disagree, that it would be beneficial to have a professional job title that is recognised by the UK Cyber Security Council?

Question 15a. Please explain more about why you agree or disagree that it would be beneficial to have a professional job title recognised by the UK Cyber Security Council.

Question 16. As an employer, would you be willing to pay more (in terms of wage) for someone who has an assessed competency based on a regulated professional title?

Question 17: How much more may you be willing to pay in terms of annual wage for someone who has an assessed competency based on a regulated professional title?

Question 18: As an employer, would you pay more (in terms of training and professional development) for someone who has an assessed competency based on a professional title awarded by the UK Cyber Security Council?

Question 20. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that there should be a centrally-held Register of Practitioners for the cyber profession?

Question 21. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that the Register of Practitioners should include a periodic review to ensure practitioners continue to meet competence and ethical requirements?

Fully agree

Question 22. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that employers should not be legally required to employ practitioners whose titles have been recognised through the UK Cyber Security Council?

Fully agree

Question 24. To what extent would it be helpful or unhelpful, ranging from very helpful to very unhelpful, to explore introducing public procurement routes to embed competency requirements for the market, as it relates to cyber professionals?

It is not entirely clear what is entailed here. If regulation is adopted then it is vital that the public sector understands the requirements and the system of regulation and that public procurement rewards those who seek to engage positively with the system and does not readily support those who do not. That should include using public procurement to drive the adoption and uptake of the new system. If people feel that they can ignore the system and still win public sector work, then it

totally undermines the message implied in the introduction of regulation. If its important enough to regulate then the public sector should then prioritise purchasing from those who are regulated.

Question 25. To what extent do you agree or disagree, ranging from fully agree to fully disagree, that government departments and relevant public sector bodies should align recruitment and professional development standards to those developed by the UK Cyber Security Council?
Mostly agree – although as noted in the summary it is not just about the Council – its about the public sector recognising professional qualifications in other safety critical roles and requiring those working in those areas to be recognised by the relevant professional bodies.

Question 26. Should the government and/or the UK Cyber Security Council continue to explore the creation of a further voluntary certification scheme that is aligned to existing programmes?

Yes

Question 27. To what extent do you think it would be helpful or unhelpful, ranging from very helpful to very unhelpful, for Cyber Essentials and CCP to align their requirements with any future professional standards that may be set by the UK Cyber Security Council?

Very helpful

Question 28. In addition to the proposals mentioned in the document above, what more could be done to further support cyber security professionals and the policy ambition to embed standards and pathways within the profession?

As noted above, there is a need for government to recognise the importance of professional standards in relation to cybersecurity and other related life safety disciplines and to create a system of regulation that is coherent across the various disciplines involved.

Question 29. Do you consider there to be additional considerations required to ensure that these proposed measures will not provide unnecessary additional barriers to entry for candidates to enter and progress a career in cyber security?

Yes

Question 29a. What additional measures could be considered?

It will be important to develop an appropriate evidence base to demonstrate that individuals and teams accredited under the new system remain competent and that there is a measurable positive impact on overall systems security and no negative impact on wider life safety considerations.

END

Please do not hesitate to contact us for more information on this response.