SUMMARY OF (ISC)^2 RESPONSE TO A CONSULTATION BY THE DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT (DCMS) ON EMBEDDING STANDARDS AND PATHWAYS ACROSS THE CYBER PROFESSION BY 2025

Submitted by
Organisation: (ISC)^2

The Department for Digital, Culture, Media & Sport (DCMS) issued a public consultation in January 2022 on proposals to develop the cyber security profession in the UK. As an industry leader and the largest not-for-profit association of certified cyber security professionals in the world, (ISC)^2 took the opportunity to address the issues put forth by DCMS and provide feedback on the proposals.

Cyber security is a rapidly evolving sector. Changes in threat landscape and risk means that industry must be nimble to address the ever-changing operational environment. Legislation to protect people and organisations needs to be adaptable as well. (ISC)^2 is of the firm belief that cyber security represents a human challenge, first and foremost and that a pertinent need exists for government to provide guidance, assistance, and limited, but thoughtful regulation for both individuals and organisations within the cyber security sector with key areas of focus including strengthening and refining day-to-day cyber security management systems. (ISC)^2 believes that an organisation that can successfully improve the 'people' element will invariably improve the 'process' element as well as the 'technology' element. The outcome will be far better overall cyber security, better resiliency and will be far better prepared to prevent, detect, respond, and recover from an inevitable set of cyber security challenges. It is critical to appreciate that technology and process outcomes will always be driven by people and these outcomes will depend almost entirely on how knowledgeable, skilled, experienced, and competent people are in the cyber security sector.

An immense amount of work has already been achieved by the UK government in improving and reinforcing the need for strong cyber practices across all organisations in the UK, including setting out a comprehensive *National Cyber Strategy 2022* as well as the *Government Cyber Security Strategy: 2022 to 2030*. (ISC)^2 applauds this work and contends that while this bodes well for the future, much more remains to be achieved in the operationalisation and execution of these and subsequent strategies to ensure a safer and more secure cyber UK.

The response of (ISC)2 to the DCMS public consultation centred around three major themes.

1 - The Role of Government in The Professionalisation of the Cyber Security Workforce

(ISC)^2 contends there is an important need for government to provide guidance, assistance and considered intervention into the market in relation to defining, embedding and promoting professional standards in the cyber security sector. (ISC)^2 submits that the best place for government to achieve this will be through two specific initiatives:

- **Initiative One:** The strengthening and refining of regulatory requirements and obligations upon all organisations in relation to their day-to-day cyber security management strategies. Additionally, the adoption of strengthened regulation pertaining to an employee's level of cyber security competency specific to organisations of a certain size and nature and/or organisations holding, processing, or controlling data consisting of certain levels of sensitivity and importance.

- **Initiative Two:** The appointment of a statutorily recognised regulatory body which will serve as a facilitator and guardian of professional standards, codes of conduct and codes of ethics within the cyber security sector.

As a standards-based organisation with an international focus, (ISC)^2 welcomes efforts to establish professional standards of practice for the activities which need to be performed within the cyber security sector.(ISC)^2 notes that numerous skills frameworks, tertiary educational programs, industry-recognised accreditation, and certification programs as well as vendor certificate schemes exist in the cyber security market today. (ISC)^2 contends that the quality assurance function inherent within the BS EN ISO / IEC 17024 standard should be adopted for the purposes of granting accreditation to cyber security practitioners for the purposes of any potential recognition. From a financial perspective, (ISC)^2 believes that government is best placed to implement additional measures that support the goals of a more cyber safe and resilient UK. In the submission, (ISC)^2 advocated for the inclusion of measures such as the provision of subsidies, funding, or tax concessions for individuals and/or employers of individuals seeking the necessary training and approved certifications which will lead to candidates formally entering the profession as certified professionals.

2 - Adapting Professionalisation Models from Other Professions

(ISC)^2 firmly believes that there are exemplars in other, more mature industries that serve as useful references for how the successful embedding of professional standards could proceed in the cyber security sector in a manner that the market will understand, value and support. (ISC)^2 contends that the UK accounting sector provides such an example. The accounting profession is not formally regulated by government, nor is it overseen by any statutory body. However, there is a very strong distinction between an ‘accountant’ and a ‘chartered accountant’ with very robust and strict mechanisms that exist for individuals seeking to attain chartered accountant status. Such individuals must demonstrate knowledge, skills, experience, and competency to a satisfactory level. Most importantly, chartered accountant status is awarded by one of several recognised accounting industry bodies.

The UK accounting profession features strong industry oversight through the Financial Reporting Council (FRC). (ISC)^2 contends that there is a role for the UK Cyber Security Council to play in a very similar and highly impactful function in providing oversight, guidance and quality assurance to the cyber security sector. Additionally, under the accounting profession, there is a central role for reputable certification bodies to issue accreditation to accounting professionals. Similarly, (ISC)2 contends that under the proposed scheme, there is an analogous role for reputable cyber security certification bodies such as (ISC)^2 to provide cyber security personnel accreditation in the space under the auspices of the UK Cyber Security Council.

3 - Importance of Harmonising Standards in cyber security

(ISC)^2 argued the case in the submission that a clear and well-crafted competence framework for cyber security professionals, as described through the potential accreditation scheme under the UK Cyber Security Council, will assist the market better understand cyber security roles to hire for, and better assess candidates against that competency. In the submission, (ISC)^2 advocated for any UK-based competency framework to operate harmoniously with both existing internationally recognised skills frameworks, such as the US NIST NICE and internationally recognized SFIA and CIISec frameworks. Most critically, (ISC)^2 reiterated the call that appropriate BS EN ISO / IEC 17024 accredited cyber security certifications, such as those issued by (ISC)^2, underpin any proposed professionalisation model for the UK cyber security workforce that is operated by the UK Cyber Security Council. Furthermore,(ISC)^2 recognises that any competence framework that seeks to implement professional standards for the cyber security sector will need to be balanced with the need to ensure that any barriers to entry, either actual or perceived, do not affect an individual’s desire or decision to seek a career in cyber security.

The full (ISC)^2 submission to the DCMS consultation is available to view.