Embedding standards and pathways across the cyber profession by 2025

This publication is available at https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025/embedding-standards-and-pathways-across-the-cyber-profession-by-2025

1. Ministerial foreword

Julia Lopez MP, Minister for Media, Data, and Digital Infrastructure

The UK is a global tech leader. We have seen impressive growth, record levels of investment and a fast growing tech workforce. Cyber security is core to our success in tech. We have hundreds of successful startups, and a growing number of cyber unicorns. Investment in cyber can be seen across the whole economy, securing critical infrastructure, securing government and securing businesses.

We have amazing technology, from artificial intelligence driven systems detecting threats, to new microprocessor designs that design out malware at the silicon level. The government is determined to not just maintain this world leading position, but to accelerate the progress we are making, and make the UK more resilient against cyber attackers. We have listened to businesses and other organisations on how we can achieve this and the message is clear. The key to our continued success is people.

The government is committed to ensuring we have enough people with the necessary skills in the UK to support the tech sector and to ensure that we can manage and respond to cyber threats. Over the last year we have offered cyber skills bootcamps as part of the National Skills Fund, our Cyber Launchpad programme has helped people start their cyber career, and our schools programme, Cyber Discovery, attracted tens of thousands of participants. Many businesses, colleges and others across the country have been making impressive efforts to upskill and attract more people to the cyber profession. Yet all of these efforts still have a long way to go to address the lack of diversity in the workforce. We need a better gender balance. We need to ensure that ethnicity is not a barrier to leadership and senior roles. We need geographic diversity to ensure all our communities benefit from the growth of the cyber industry.

While we continue to draw more people into cyber careers we have not yet made it easy enough for businesses to know what specific skills they need. The term "cyber professional" encompasses many different specialisms covering those who design systems to be more secure, those who test security, those who research threats, those who detect intrusions, those who respond to incidents and many more. It is hard enough to establish what sort of specialist you need but even harder to establish if a specialist has the skills you need, and the qualifications or experience to demonstrate those skills. In March we launched the UK Cyber Security Council, the new professional body to lead the cyber workforce. The Council will make it easier for employers to identify the skills they need. The Council will also, in time, raise the bar, acting as a force to raise standards and to ensure that people working in cyber are properly equipped to protect us from criminal gangs and hostile states.

A better organised cyber profession will also make it easier to attract people, retain people and help them drive their career forward. People need a clear understanding of the pathways available to them. The UK Cyber Security Council is critical to achieving this and leading the response to increasing diversity in the workforce. By defining and standardising the professional cyber security landscape, as well as creating clearer information for young people and professionals, the UK Cyber Security Council will embed itself as the voice for the cyber security profession. To guarantee progress, we must make sure the Council is empowered.

I am publishing this consultation on the cyber security profession to further this aim. The proposals look to provide clarity within the cyber security profession as it stands, embed professional standards and pathways. This will recognise cyber as a profession similar to the more established fields such as accounting, law, and engineering. The proposals set out to provide clarity on and more easily accessible pathways into the profession. By doing this we can continue to encourage those with passion and aptitude into the cyber security profession which will be imperative for long term security and success in the UK.

We are asking for honest and open contributions to this consultation to give government meaningful insight from the perspective of those involved in all aspects of the cyber security profession. I look forward to receiving your responses.

Julia Lopez MP

Minister for Media, Data, and Digital Infrastructure

2. How to respond

We welcome your views. To help us analyse the responses please use the online system wherever possible. Visit the Department's online consultation tool to submit your response. Hard copy responses can be sent to:

Cyber Skills and Professionalisation Team
Department for Digital, Culture, Media & Sport
4th Floor
100 Parliament Street

London
SW1A 2BQ

cyberlearning@dcms.gov.uk

The closing date for responses is Sunday 20 March 2022 at 11.45pm.

When providing your response, please also provide contact details - we may seek further information or clarification of your views.

Copies of responses, in full or in summary, may be published after the consultation closing date on the Department's website.

2.1 Freedom of information

Information provided in the course of this consultation, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 2018 (DPA).

The Department for Digital, Culture, Media and Sport will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK government's consultation principles.

If you want the information you provide to be treated confidentially, please be aware that, in accordance with the FOIA, public authorities are required to comply with a statutory code of practice which deals, amongst other things, with obligations of confidence.

In view of this, it would be helpful if you could explain to us why you wish that information to be treated confidentially. If we receive a request for disclosure of that information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances.

2.2 Privacy notice

This privacy notice explains your rights and gives you the information you are entitled to under the Data Protection Act 2018 and the UK General Data Protection Regulation ("the Data Protection Legislation").

2.3 Who are we looking to engage with?

We are keen for as broad a range of interested parties as possible to engage with and respond to this consultation. This includes, but is not limited to:

- current cyber security professionals
- current cyber security apprentice and those on employer graduate programmes

- current or prospective employers of, or consumers of services provided by cyber security professionals in the UK
- existing cyber security professional organisations, including certification and qualification providers
- individuals who aspire to work in cyber security in the UK
- public sector bodies including but not limited to local authorities and health services
- private businesses with an interest in cyber security including small and medium-sized enterprises (SMEs)
- students, recent graduates and adults mid-career who are thinking about cyber security as a career
- academia and educational establishments
- other professions which interrelate with existing cyber security professional organisations
- law enforcement community
- practitioners across a range of sectors including insurance, finance and retail
- employers or practitioners in critical national infrastructure (CNI) roles
- membership and regulatory bodies and any other organisations with an interest in cyber security in the UK

3. Executive summary

The cyber profession is nascent and has developed over the last generation, drawing on multiple specialisms, many of which have origins across other professional structures in science, law and engineering. It has now reached a level of maturity where it needs its own identity, shape and form.

DCMS undertook a public consultation exercise in 2018 which helped identify the characteristics of the profession and the need for a body to form this new identity. Through this, DCMS funded the creation of the UK Cyber Security Council, which launched in March 2021. Government will look to this body as the authority on the cyber profession, bringing together the existing work of professional and certifications organisations in this space, to meaningfully communicate and assure consistency across standards and pathways.

This Council will need to succeed if wider government and industry ambitions to address the scale and diversity of the skills shortage are to be met. We are now at the next stage of policy development, whereby we are considering how best to ensure that the UK Cyber Security Council is suitably empowered to be the voice of the profession. We are keen for the Council to build governance and establish its leadership, and through which wider partnership can achieve and embed clarity in the profession. This consultation seeks views on the most effective means of doing this over the next strategic period between 2022-2025.

The rationale for intervention has been set out and challenged through stakeholder engagement across employers, practitioners and both academic and professional stakeholders. Throughout, we have been clear to balance the need to quality assure those practising within cyber security, while also not providing unnecessary barriers to entry and progression.

We are presenting proposals around the role of legislation to underpin the role and reach of the UK Cyber Security Council. This will allow for the Council to develop a common taxonomy that recognises expertise across the range of specialisms in the field, and formally recognise its role as standard-setter. There are further considerations put forth as to how the government can lead by example in this space, through non-legislative levers, such as requirements around procurement and broader alignment on recruitment across government and wider public sector cyber roles.

Depending on the outcome of this consultation, these proposals will inform wider policy focus to contribute to the ambitions set out in the Integrated Review of Security, Defence, Development and Foreign Policy and the recently published National Cyber Strategy 2022.

4. Introduction

The Integrated Review of Security, Defence, Development and Foreign Policy set out the strategic goal of cementing the UK's position as a responsible and democratic cyber power. Central to the UK's ambitions will be a sustained supply of diverse and high quality individuals into the cyber workforce, capable of making systems more resilient against cyber threats, as well as innovating and developing new approaches to capitalise on the opportunities of cyberspace more broadly.

The size and scope of the challenge to achieve this ambition is clear. We know that there is an annual shortfall of 10,000 professionals entering the UK cyber workforce.[footnote 1] This exacerbates the existing diversity shortcomings of the profession, with only 16% of the cyber sector workforce being female. We know that this is lower than other digital and tech sectors. Alongside this, there is also evidence that organisations are struggling to recruit effectively and this has a direct impact on their cyber capability.

We know that 50% of all UK businesses across the economy have reported a basic technical cyber skills gap within their organisation, while 37% of all vacancies advertised within the cyber sector have been hard to fill due to the candidate lacking technical skills and knowledge. Organisations have, as a result, reported that almost 9 in 10 cyber functions have been absorbed into non-cyber security roles, making it more difficult to track competency demonstration.[footnote 2]

Addressing this problem requires multiple focuses around ensuring that interested young people are inspired towards this career, existing workforce professionals from outside cyber security are supported into this field and a specific focus on supporting individuals from underrepresented groups and disadvantaged backgrounds. To this end, there are a range of government and industry initiatives that look to increase the number and diversity of people entering cyber security jobs across both the cyber sector and the wider economy. This includes inspirational activity through the NCSC Cyber First portfolio of programmes, as well as skills bootcamps funded through the recent National Skills Fund.

However, we know that there is also a bespoke need to address the feedback we have heard from practitioners and industry through the 2018 public consultation on developing the cyber security profession. This highlighted that

navigating a career in this field remains difficult and the ability of employers to assess competence through recruitment is inconsistent. Cyber security is a complex, nuanced and increasingly established profession that needs to be recognised in its own right. This field is layered with multiple specialisms, across which a professional's responsibilities can currently incorporate a number of cyber functions.

This was drawn out in a previous consultation on the cyber security profession in 2018, which identified the following challenges:

- Misconceptions and stereotypes about cyber security professionals remain and many still consider cyber security to be a career which lacks clear routes into and through.
- The current qualification and certification landscape is hard to navigate, making it difficult to assess the options available and make appropriate, informed choices about career paths or the skills that an organisation requires.
- Linked to this, many existing professional organisations are unable to articulate the equivalence of their qualifications or certifications in the absence of a common technical framework.
- To build on the excellent work these organisations do, we heard better coordination and articulation of how their work interrelates would mean it could have a greater collective impact.
- There was no widely recognised and authoritative voice to coordinate and corral views from the whole breadth of the cyber security profession.
- In attracting the next generation of cyber security professionals, there is a range of excellent outreach initiatives, across government and the private sector, but these can sometimes be hard to find or the choice confusing and overwhelming.
- New legislation and new technologies, of which cyber security is a core part, make these challenges even more pronounced and pressing to address.

To address these challenges, the creation of the UK Cyber Security Council was funded by DCMS to drive standardisation of the professional landscape which unlocks efforts to scale impact and meaningfully address diversity shortcomings in the workforce. This was delivered by a consortium of professional and certification organisations, led by the Institution of Engineering and Technology. This body was launched in March 2021.[^3.

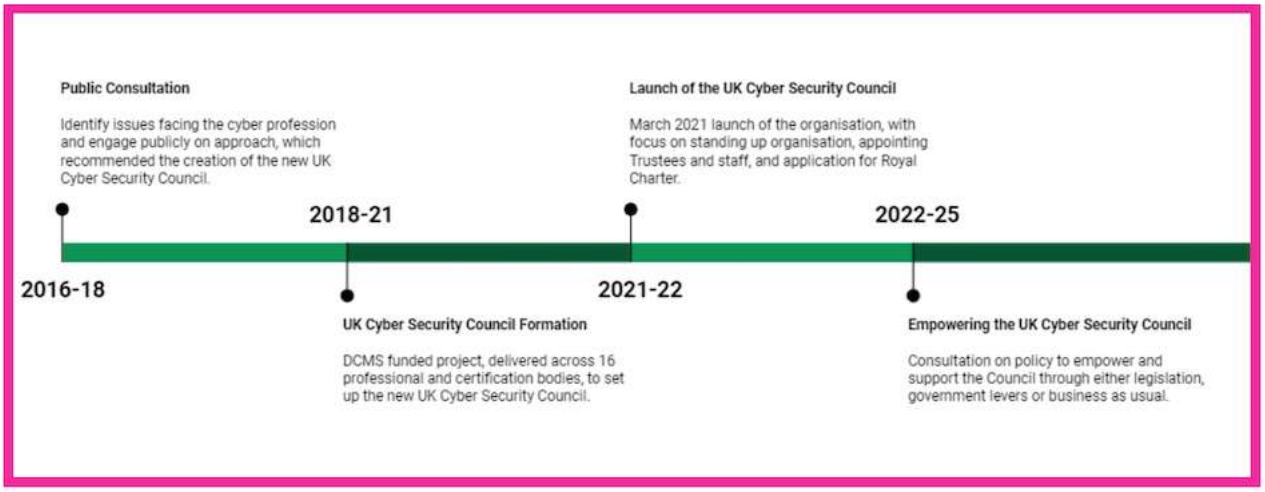

Figure 1: Timeline of profession policy development

We are now at the next step of policy development and exploring how to most effectively empower the Council to lead the profession and set clear and comprehensive professional standards and pathways. If the UK Cyber Security Council, and the breadth of professional bodies that we anticipate will form its membership, is not suitably supported then the challenges in the profession will persist.

When considering next steps, we have looked to draw parallels from established professions already in place, such as law, engineering and medicine - where the professional structure provides recognition of and confidence in a practitioner's experience and suitability for a specific need. It is clear that the focus of the next strategic period will need to strengthen the Council and its professional standards and pathways. This is alongside establishing the clear drivers for practitioner and employer pick up, and ensuring clarity in the taxonomy used across the profession.

There are a number of approaches to be considered as to how this can be done most effectively and, through this consultation, we are keen to gather as many views as possible on how next steps should be meaningfully taken to assure the quality of the profession. We are keen to ensure that we have the right professional standards and mechanisms in place to ensure that people with the right skills are identified as competent to manage the UK's cyber risk, without providing unnecessary barriers to entry and progression for professionals.

Alongside this document, the consultation survey sets out a series of questions around these proposals. These aim to ensure all interested stakeholders can provide a view and opinion as to the rationale for the approach, while exploring the potential impact of the proposals on both the current and future workforce.

5. Context and rationale for intervention

The use of technology in everyday life continues to grow, with more individuals and businesses going online, and this has been accelerated by the pandemic. [footnote 4] The attack surface available to cyber criminals continues to grow, yet many of the threats faced by the economy today are based on vulnerabilities that have been around for many years and relate back to the design of long established technologies. These vulnerabilities often relate to buffer overflow, SQL injection, weak passwords and configuration that is not fit for purpose. While technology continues to change and be innovative, many of the fundamental ways it is exploited have not and with that, the means through which these risks can be mitigated remain consistent.

We see that there are more cyber attacks targeting these vulnerabilities given the increased number of users and businesses online. There is of course a role to communicate best practice across the workforce more broadly focusing in on human error, but there is also a need to ensure practitioners are equipped with the necessary level of knowledge, skill and experience to support their organisation.[footnote 5] This will range across numerous specialisms within the cyber profession and incorporate the varying requirements of both technical and non-technical skills.

What do we want to achieve?

We need to ensure that the UK has the right professional standards and mechanisms in place to recognise individuals who are competent and sufficiently expert, as required, to manage the UK's cyber risk. This is essential for assuring that practitioners responsible for cyber security functions that include the design, testing, monitoring and reacting to system breaches, have the right knowledge and skills to do this effectively.

Through the Cyber Security Breaches Survey 2021, we know that 77% of businesses and 68% of charities consider cyber security a high priority. However, skills within this area were poorly understood and undervalued amongst both management boards and IT teams. This is consistent with what we have heard more broadly around the need for this complex profession to be better defined to support employers in this regard. In the meantime, there is additional emphasis on cyber professionals to influence behaviour and culture within their organisations. This reliance on practitioners needs to be balanced with clarity on the precise specialist know-how that they can provide, and mitigate an over-reliance on an individual to be responsible for all cyber security practice.

We know employers face challenges in understanding what knowledge, skill and experience they require from candidates and navigating the myriad of certifications and qualifications on offer. This impacts on effective recruitment and allocation of cyber security responsibilities within an organisation. This consultation is specifically focused on how we can more readily recognise expert practitioners and embed a clear understanding of what practitioners need to know and be able to demonstrate. However, this approach will align and complement broader efforts to boost the number and diversity of individuals entering the cyber workforce.

Government focus on cyber profession: NCSC and MoD

The National Cyber Security Centre - which is a part of GCHQ and is the UK's national technical authority for cyber security - has, over the last five years, developed a number of initiatives that establish knowledge, quality assured learning and assess professional competence from the perspective of the National Technical Authority. These were done as a result of the gaps present across existing qualifications in a number of specialisms. These products include the Cyber Certified Professional (CCP) accreditation, recognising those who demonstrate an ability to apply their critical skills and knowledge in real world situations and NCSC-Certified Degrees, which allow students and employers to identify high quality cyber security education at Levels 6 and 7, including undergraduate and postgraduate Master's degrees and degree apprenticeships.

The Ministry of Defence and the National Cyber Force are significant stakeholders across cyber space - in both defensive and offensive activity - and are particularly active across broader training and professionalisation focuses. This includes the work of the Defence Cyber School and the broader consideration around standards and pathways that inform and underpin efforts in this area.

Up to this point, we know that the professional landscape and training market have produced learning and training quality products that meet aspects of this need. Now, the UK government are looking to the new UK Cyber Security Council to bring together the range of existing activity and best practice. [footnote 6] We expect this body to hone the work of the profession and bring together the existing qualification and certification market under a coherent structure. Through this, providing an authoritative viewpoint of the specialisms that exist and the bodies that can collate and quality assure the practitioners working within these fields.

This work includes the development of a Career Pathways Framework, [footnote 7] using existing products such as the Cyber Security Body of Knowledge and work undertaken by Skills Development Scotland. The UK Cyber Security Council's application for a Royal Charter that will support its ambition to award a bespoke chartered status recognising cyber security professional expertise and excellence throughout the workforce, building on and aligning with existing professional qualifications and certifications.

However, at this point in time, all these requirements remain voluntary and uptake is dependent on practitioners and employers recruiting these professionals. Currently, increasing awareness of this requirement is down to the UK Cyber Security Council and its membership to achieve. The consultation is seeking views on the value additional government support can have in this space and what it looks like.

6. Proposal of considerations

We are now at the stage of policy where we need to consider how to most effectively embed the professional standards defined and recognised by the UK Cyber Security Council. We have engaged broadly with industry, professional

and academic representatives to assess what is the role of the government in achieving this most effectively.

The first consideration is around the need for government intervention, beyond continuation of initial support to ensure that the UK Cyber Security Council stands up and establishes itself as a sustainable and credible organisation over the next strategic period. The government is supporting the Council with:

- grant funding for its first four years of operation to allow it to develop a business model and membership base to make it self funding
- support for its recent application for Royal Charter status
- support by committing to align the government cyber profession with the standards and frameworks developed by the UK Cyber Security Council
- support by transferring responsibility for relevant cyber security standards, when the Council reaches the necessary level of development, from government, to the UK Cyber Security Council

This level of support should send a clear signal to organisations across the economy that the government approves of UK Cyber Security Council standards and that these standards should be applied when seeking to build organisational resilience against cyber threats. We are concerned, however, that this is not a foregone conclusion. This approach has been undertaken previously in this space and has not achieved the intended objective of embedding professional standards and pathways. As a result, we do not think that is a sufficient approach to achieve the outcomes required and address the underlying needs of the profession that were identified through the 2018 public consultation.

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 2a. [If mostly or fully disagree] Please expand on the reasons for this response.

[Open-ended question]

If further active government intervention is required, we must now explore whether this should be legislative or non-legislative in nature, or a combination of both. A legislative scheme would be mandatory whereas a non-legislative scheme would typically be voluntary. If legislation were the preferred option, we have considered what this could look like and fit with the maturity of the profession over the next three years.

We have explored this legislative option from the broadest point of view and honed down to what is deemed a realistic and achievable means for embedding legislative underpinning for the cyber profession. We do not deem wider regulation for all cyber security functions, held and enforced by a single regulatory body to be appropriate at this time. This is due to the potential impact that might have on exacerbating existing skills shortages and diversity shortcomings of the profession. Additionally, there is a need to ensure legislation supports and encourages regulators from particular sectors to work with the Council to ensure the relevant professional standards and pathways are appropriate for their specific needs.

We have heard through engagement that providing recognition of the UK Cyber Security Council through legislative underpinning would further support its role as the standard setting body for the profession. This would mean the formal recognition of the body as the designated authority on the cyber profession, in line with similar standing for a range of professional bodies across the economy.[footnote 8] This narrative is already clearly articulated through broader DCMS and cyber skills strategic direction, and legislative backing may be appropriate to reinforce this. This legislative underpinning would only be required if there is a statutory scheme to regulate.

Consultation questions

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 3a. [If mostly or fully disagree] Please expand on the reasons for this response?

[Open-ended question]

As part of this question, consideration needs to align to the broader question of whether there is a need to regulate cyber professionals under a legislative (mandatory) scheme and how this can be done. This will have to balance the need to avoid additional barriers to entry and progression for a workforce that is already experiencing a skills shortage, but also mitigating the risk that under-qualified practitioners could carry out essential cyber security functions such as Penetration testing, Cyber Risk Management, Incident Response and Management and Cyber Security Architecture.

We have considered what would be required to introduce statutory regulation by activity under a specific legislative scheme. This would mean certain roles, at least initially, would have to be prioritised. Professionals regarded as under-qualified would be prohibited from carrying out activities related to essential cyber security functions and would need to be assessed via the UK Cyber Security Council before being permitted to practice. A definition of an under-qualified professional would be provided by the UK Cyber Security Council.

There would be a further question on the extent to which regulation by activity would need to be sector or industry specific, and how this would be enforced. We know there is precedent in the engineering profession, as certain areas, largely safety related, are reserved for engineers recognised by the Engineering Council and enforced through specific legislation. This is considered to be a point that may have merit in the future, but currently is assessed to be too early to consider without further evidence. We propose that this question should be considered in future policy development.

To note, questions 4 onward are seeking to explore what a proposed legislative scheme would look like and consider in practice.

Consultations questions

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Alongside this, we have considered statutory regulation by professional titles and consider this option to be more viable and appropriate to achieving the outcomes required for the cyber profession. In particular, this would ensure that roles - which are inconsistently defined and recruited for across employers - have coherence that can be assessed more easily by prospective entrants to the profession, existing practitioners and employers.

This regulation would result in individuals having to meet competency standards set by the UK Cyber Security Council, before they can utilise a specific professional job title across the range of specialisms in cyber security. However, this would not result in individuals being prohibited from undertaking activities under a job title if they chose. This would also prioritise a transition period up to 2025 for existing practitioners to ensure they are afforded an appropriate and fair amount of time, in line with this approach. This is seen as a suitable balance between embedding clear definitions and a common taxonomy, while also not preventing individuals from practicing in a field that is experiencing a significant skills shortage.

Consultation questions

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 agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- No
- Do not know

Question 7a. [If yes] what additional measures should be considered?

[Open-ended question]

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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 agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree

- Mostly disagree
- Fully disagree
- Do not know

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

- Yes
- No
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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.

[Open-ended question]

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?

- Yes
- No
- Do not know

Question 17: [if yes] 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?

- £1,000 or less
- Over £1,000 to £4,000
- £4,001 to £7,000
- £7,001 to £10,000
- Over £10,000
- Do not know

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?

- Yes
- No
- Do not know

Question 19: [if yes] How much more may you be willing to pay in terms of training and development for someone who has an assessed competency based on a professional title?

- £500 or less
- Over £500 to £1,000
- Over £1,000 to £5,000
- Over £5,000
- Do not know

As part of this, we know that there has been consideration of the value of a Register of Practitioners, similar to what exists in the medical and legal professions. This would set out the practitioners who have met the eligibility requirements to be recognised as a suitably-qualified and ethical senior practitioner under a designated title award. This may include periodic reviews stipulated by the UK Cyber Security Council to ensure practitioners continue to meet competence and ethical requirements. Employers would not be legally required to employ practitioners whose title has been recognised through the UK Cyber Security Council, but encouraged to do so.

Consultation questions

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- Mostly agree
- Neither agree nor disagree
- Mostly disagree

- Fully disagree
- Do not know

Question 22a. [If disagree] Why do you think that employers should be legally required to only employ practitioners whose titles have been recognised through the UK Cyber Security Council?

[Open-ended question]

We have heard the need for legislation in this area to underpin and embed professional standards and pathways, however it is not the single means of meeting broader ambition and managing cyber risk effectively across the UK. This will need to ensure it complements and aligns with legislative ambitions around products and organisations. This includes (i) legislation being developed that looks to mandate important cyber security measures for connected products, to protect the consumer; and (ii) the work of the Network and Information Systems Regulations to ensure that appropriate organisations are taking the necessary steps to ensure the resilience of essential services to the economy.

This route does open up potential opportunities to underpin and align with existing legislative frameworks. We know, at the time of writing, that there is work being explored around potential reform of the Computer Misuse Act. While this work is a separate process upon which no link can be fully defined at this point, there is potential to ensure a prominent role for defined professional competence to expand the scope of what changes may be possible where considered appropriate to ensure professionals are sufficiently clear on the legal confines of their activity.

We consider that skills is a devolved matter and any proposed legislation is likely to initially be England only. However, we will continue to work with the devolved administrations to understand overlap and complementarity to legislation as appropriate.

Consultation questions

Question 23. Do you consider there to be any perceived risks or overlaps with existing legislative arrangements, particularly in devolved nations?

- Yes
- No
- Do not know

Question 23a. [If yes] In what areas do you think there would be perceived risks or overlaps with existing legislative arrangements?

[Open-ended question]

Alongside the legislation considerations, we have engaged broadly on the non-legislative measures that the government can do to complement wider legislation if this was progressed. This included consideration of the levers the government should explore to increase the use of professional standards and pathways, which can be referenced by relevant regulators, Lead Government Departments and Competent Authorities.

We have identified two primary points of focus to align and progress over the next strategic period to 2025. This includes government procurement requirements and exploring the extent to which a similar demonstration of competence that aligns to the standards set by the UK Cyber Security Council should be required for specific government functions. Further, the government and broader public sector is a major employer of cyber security professionals. We have heard that government departments and public sector bodies should align recruitment and professional development standards to those developed through the UK Cyber Security Council.

Consultation questions

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?

- Very helpful
- Slightly helpful
- Neither helpful nor unhelpful
- Slightly unhelpful
- Very unhelpful
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Finally, we have heard that further voluntary certification schemes to help build momentum of this work may be explored and built on existing programmes such as the Certified Cyber Professional (CCP) scheme delivered through NCSC. This would also include aligning the Cyber Essentials scheme which supports organisations to implement the baseline security requirements needed to ensure UK businesses are increasing their resilience to cyber attacks and data breaches.

Consultation questions

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
- No
- Do not know

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
- Slightly helpful
- Neither helpful nor unhelpful
- Slightly unhelpful
- Very unhelpful
- Do not know

We propose that this combination of focuses should inform policy ambition over the next strategic period 2022-2025, and progress towards the ambition to embed the coherent and universally recognised set of professional standards and pathways to be set by the UK Cyber Security Council. We will build an evidence base over the same period to understand where there may be a well-articulated need for further requirements and licencing consideration to practice across certain specialisms, and across certain sectors and industries. We intend to consider this within the scope of legislative need in the future, but do not consider this an appropriate or proportionate intervention for now.

Consultation questions

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?

[Open-ended question]

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
- No
- Do not know

Question 29a. [If yes] what additional measures could be considered?

[Open-ended question]

7. Next steps

This public consultation provides the opportunity for us to obtain views and considerations from all stakeholders with an interest in the cyber security profession and informing the next steps of government policy. We encourage anyone with an interest in this area to engage and respond. The consultation will be open from Wednesday 19 January 2021 until 11.45pm on Sunday 20 March. The government will publish a response in due course.

8. Appendix - full list of 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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 2a. [If mostly or fully disagree] Please expand on the reasons for this response. [Open-ended question]

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 3a. [If mostly or fully disagree] Please expand on the reasons for this response? [Open-ended question]

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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 agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- No
- Do not know

Question 7a. [If yes] what additional measures should be considered? [Open-ended question]

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree

- Fully disagree
- Do not know

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 agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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

- Yes
- No

- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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. [Open-ended question]

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?

- Yes
- No
- Do not know

Question 17: [if yes] 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?

- £1,000 or less
- Over £1,000 to £4,000
- £4,001 to £7,000
- £7,001 to £10,000
- Over £10,000
- Do not know

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?

- Yes
- No
- Do not know

Question 19: [if yes] How much more may you be willing to pay in terms of training and development for someone who has an assessed competency based on a professional title?

- £500 or less
- Over £500 to £1,000
- Over £1,000 to £5,000
- Over £5,000
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

Question 22a. [If disagree] Why do you think that employers should be legally required to only employ practitioners whose titles have been recognised through the UK Cyber Security Council?

[Open-ended question]

Question 23. Do you consider there to be any perceived risks or overlaps with existing legislative arrangements, particularly in devolved nations?

- Yes
- No
- Do not know

Question 23a. [If yes] In what areas do you think there would be perceived risks or overlaps with existing legislative arrangements?

[Open-ended question]

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?

- Very helpful
- Slightly helpful
- Neither helpful nor unhelpful
- Slightly unhelpful
- Very unhelpful
- Do not know

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?

- Fully agree
- Mostly agree
- Neither agree nor disagree
- Mostly disagree
- Fully disagree
- Do not know

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
- No
- Do not know

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
- Slightly helpful
- Neither helpful nor unhelpful
- Slightly unhelpful
- Very unhelpful
- Do not know

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?

[Open-ended question]

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
- No

- Do not know

Question 29a. [If yes] what additional measures could be considered?

[Open-ended question]

Demographic questions

DQuestion 1. Are you responding as an individual or on behalf of an organisation?

- Individual
- Organisation

DQuestion 2. [if individual] Which one of the following statements best describes you?

- Current or prospective employer of cyber security professionals
- Current cyber security professional
- Current cyber security apprentice and those on graduate programmes
- Consumer of services provided by a cyber security professional
- Law enforcement community
- Practitioners in insurance
- Professional in another sector
- Academic
- Student with an interest in a career in cyber security
- Interested in a career in cyber security
- Interested member of the general public
- Other

DQuestion 3. [if organisation] Which of the following statements best describes your organisation? (Select all that apply)

- Organisation that employs, contracts or uses cyber security professionals
- Cyber security training provider and or certification/qualification provider
- A cyber security professional body
- Other form of cyber security professional organisation
- An academic or educational institution
- Non-cyber security specific professional body or trade organisation with an interest in cyber security
- Membership body
- Public sector body including but not limited to local authorities and health services
- Law enforcement community
- Other

DQuestion 4. [if organisation] Which one of the following best describes the sector of your organisation?

- Cyber security
- Production / Manufacturing
- Distributor / Wholesale / Retail

- Telecom providers
- Information & communication technology (ICT)
- Health
- Critical National Infrastructure and National Security - please specify additional details
- Transport & Storage (inc. postal)
- Finance & insurance
- Property
- Construction
- Business administration & support services
- Education / Academia
- Public administration & defence
- Arts, entertainment, recreation
- Agriculture, forestry & fishing
- Civil society
- Accommodation & Food services
- Other services - please specify

DQuestion 5. [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.

- Under 10
- 10–49
- 50–249
- 250–999
- 1,000 or more

DQuestion 5a [if organisation] If you are a UK based company but have offices and staff in other geographical locations, how many cyber security staff work for your organisation outside of the UK

- Not applicable as all cyber security staff are UK based
- Under 5
- 5 - 10
- 11- 16
- 17-22
- 23-28
- 29 or over

DQuestion 5b. [if organisation and select option in question above] Please list which countries your cyber security staff are based in?

[Open-ended Question]

DQuestion 6. [if organisation] What is the name of the organisation you are responding on behalf of?

[Open-ended Question]

DQuestion 7. [if organisation] What is your role within the organisation on behalf of which you are responding?

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Director of Security

- Head of Cyber Security/Information Security
- Other cyber security role
- Business owner
- Chief Executive (CEO)/Managing Director (MD)
- Trustee/treasurer/on trustee board
- Other senior management role (e.g. director)
- General manager (not a director/trustee)
- PA/secretary/administrator
- Public and or government relations
- Other

DQuestion 8. Do you currently hold responsibility for hiring cyber security staff?

- Yes
- No

DQuestion 9. Are you happy to be contacted to discuss your response?

- Yes
- No

DQuestion 10. [If yes] Please provide a contact name below.

[Open-ended question]

DQuestion 11. [If yes to Q9] Please provide a contact email address below.

[Open-ended question]