Department for
Digital, Culture,
Media & Sport

IMPLEMENTING THE NATIONAL CYBER SECURITY STRATEGY - DEVELOPING THE CYBER SECURITY PROFESSION IN THE UK

GOVERNMENT RESPONSE TO PUBLIC CONSULTATION

PUBLISHED ON 21 DECEMBER 2018

CONTENTS

MINISTERIAL FOREWORD

Since the publication of the National Cyber Security Strategy (NCSS) there has been a significant increase in malicious cyber activity globally from hostile nation states and cyber criminals. As our reliance on technology grows, the opportunities for those seeking to attack and compromise our systems and data will continue to increase, along with the potential impact on individuals, organisations and the wider economy.

That is why cyber security remains a top priority for the government - it is central not only to our national security but also fundamental to becoming the world's best digital economy. It is crucial that we seek to ensure that the UK has the cyber security capability it needs to maintain its resilience to cyber threats. Government's ambition, as set out in the Initial Cyber Security Skills Strategy[1], is to increase cyber security capability across all sectors to ensure that the UK has the right level and blend of skills required to maintain our resilience to cyber threat and be the world's leading digital economy.

A key strand of that work is developing the cyber security profession in the UK. DCMS published a consultation over the summer which set out bold and ambitious proposals to drive forward the profession, including creating a new UK Cyber Security Council for the UK. The consultation received over 300 responses. This represents excellent engagement and I am extremely grateful to everyone who engaged and responded so constructively.

We have considered each response carefully and this government response sets out our analysis, conclusions and next steps. There will be further opportunities to engage in policy development through the Cyber Security Skills Strategy which is being published in parallel.

MARGOT JAMES MP
MINISTER OF STATE FOR DIGITAL AND THE CREATIVE INDUSTRIES

[1] https://www.gov.uk/government/publications/cyber-security-skills-strategy

EXECUTIVE SUMMARY

Introduction
Government published a public consultation on 19 July 2018 with proposals to accelerate the development of the cyber security profession in the UK. The proposals defined a series of objectives focused around professional development, professional ethics, thought leadership and influence for the profession, and outreach and diversity. The consultation recommended the creation of a new, independent UK Cyber Security Council to coordinate delivery.

Engagement
The consultation was open for approximately six weeks and received over 300 responses from across the cyber security community. 76% of responses were from individuals and 24% from organisations.

Analysis
The consultation document set out 14 substantive questions to explore government's understanding of the challenges facing the profession, the proposed objectives and the proposal to create a UK Cyber Security Council. There was a mix of quantitative questions with multiple-choice answers and qualitative questions with the opportunity for free text responses.

On the challenges, many respondents used the free text opportunity to broadly endorse the government's assessment. Other key themes identified were increasing cyber security understanding at board level and the need to strike a balance between increasing trust and standards in the profession while also not inadvertently preventing or dissuading new entrants from entering it. Some respondents noted there were challenges around taxonomy and definitions used in cyber security.

Almost 70% of respondents thought the Council model was an appropriate way of delivering on the proposed objectives. 41% respondents said they either disagreed or strongly disagreed that it was viable for the Council to become self-sustaining without government funding by 2021. There were a range of constructive responses in follow-up free text questions about the financial model and attributes the Council could have.

In response to the quantitative questions about the four objectives, between 70-80% of respondents supported the proposals. This included creating a chartered standard for cyber security professionals and a Code of Ethics agreed across the profession.

Conclusions

We believe the responses to the consultation represent strong support for the main thrust of the proposals - which is to define a series of objectives and to create a new, independent UK Cyber Security Council to coordinate delivery. We therefore intend to proceed to identify a lead to design and deliver the UK Cyber Security Council.

The responses to the consultation helped significantly refine and finesse our thinking and add an extra layer of granularity to our proposals. We have used that to define core criteria against which applications to lead the design and delivery of the Council will be assessed.

One of the key areas where the proposals have been refined is around implementation of the Council. There were reservations about the extent to which the ambition for the Council can be delivered in the timescales and in a way that ensures the Council is financially self-sustaining beyond 2021. We have set out firmer proposals to ensure the Council has a clear value proposition and how the consultation has helped shape other issues such as prioritisation of objectives and the proposal for Chartered Status for cyber security professionals.

Next steps

This government response is being issued in parallel with an invitation to apply for government funding to lead the design and delivery of the UK Cyber Security Council. This is being issued as a competitive process. All proposals will be evaluated against published criteria and requirements, and an assessment made to select one successful proposal. The original consultation document set out that if we did proceed to this stage, it was likely proposals would need to show they can command broad support across the cyber security professional development landscape and wider cyber ecosystem. We believe the outcomes of the consultation endorse that and it remains the key principle for the funding competition.

INTRODUCTION

The National Cyber Security Strategy (NCSS) 2016-2021 sets out the Government's ambition to ensure there is a sustained supply of the best possible home-grown cyber security talent. One of the key initiatives to deliver is defined as:

> "*developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy"*

On 19 July 2018 government published a public consultation with proposals to implement this initiative and accelerate the development of the cyber security profession in the UK. The proposals were designed to ensure the profession more coherently encourages a broader range of people with the right capabilities to enter a career in cyber security, as well as helping existing professionals have their skills and expertise recognised more easily and in a clear and consistent way. The proposals also focused on helping employers and consumers have more confidence in the professionalism, capability and integrity of those they employ or those who provide cyber security services.

The consultation was open for approximately six weeks over the summer. We received over 300 responses from a broad range of interested groups and individuals including cyber security professionals, existing professional organisations, students, employers from a range of sectors, and academia. We are very grateful to all respondents for taking the time to respond.

This document, which constitutes the government response to the consultation, provides an overview of engagement with the consultation and a summary of data received in response to each consultation question. This includes the key themes from the free text qualitative questions. We then set out our conclusions and next steps.

ADDITIONAL BACKGROUND

The consultation was issued on 19 July 2018 and closed at 17:00 on 31 August 2018. We accepted a number of written responses in the week following the formal closure of the consultation. This government response was published on 21 December 2018.

Enquiries: For questions on how to engage with the government response, or on the competitive process that is being issued in parallel, you can contact the team on: csprofession@culture.gov.uk. Alternatively you can write to the team at FAO Cyber Security Profession consultation team, Cyber Security, DCMS, 100 Parliament Street, SW1P 2BQ.

Additional copies: Additional copies are available electronically and can be downloaded from GOV.UK DCMS consultations.

OVERVIEW OF ENGAGEMENT WITH CONSULTATION

The consultation was open from 19 July 2018 until 31 August 2018. There were **307** meaningful responses. A meaningful response is considered to have answered at least one of the substantive questions posed in the consultation document and explicitly agreed to disclosure of answers. There were additional responses recorded through our online portal which had not progressed beyond the initial identifier questions, so there was no information contained to analyse.

- Of the 307 responses, 232 (76%) responses were from individuals and 75 (24%) were from organisations (cyber security employers, professional organisations etc).

- Of the 75 responses from organisations, 11 identified themselves as a “Cyber security certification/qualification provider”, 24 as an “Organisation that employs, contracts or uses cyber security professionals”, 18 as “Other”, 5 as an “Other form of cyber security professional organisation”, 7 as an “Organisation with an interest in cyber security”, 4 as “A cyber security professional body”, 2 as “An academic institution” and 1 as a “Cyber Security training provider”.

- Of the 232 responses from individuals, 173 identified themselves as a “Cyber security professional”, 14 as an “Employer of cyber security professionals or consumer of services provided by a cyber security professional”, 8 as a “Student with an interest in a career in cyber security”, 25 as “Other” and 12 as a “Professional in another sector with an interest in changing career into cyber security”.

- We asked respondents how they heard about the consultation. 81 respondents said ‘Saw an article about the survey in the media/online’, 56 respondents said ‘Engaged by Department for Digital, Culture, Media and Sport/National Cyber Security Centre/another government department during policy development’, 40 respondents said ‘Discovered survey on gov.uk while browsing’, 127 respondents gave ‘Other’ as a reason and 3 respondents did not answer the question.

- The consultation was published on gov.uk and respondents were asked to use the online portal to provide answers. The feedback we received on the

process for engaging with the consultation was broadly positive. However, a number of respondents flagged issues with the online portal, particularly the ability to click through to the end of the survey without being able to then go back to fill in earlier parts. Where respondents had difficulty with the online portal, or where requested, we accepted a Word version of the online portal questions. Where respondents sent additional information or evidence, we have not considered that as part of the responses to the consultation.

SUMMARY OF RESPONSES TO CONSULTATION

This section provides a factual summary of responses to each question in the consultation. The questions were a mix of quantitative with multiple-choice answers and qualitative with the opportunity for free text responses. We have set out the summary of the multiple-choice responses below, with graphs illustrating the spread of answers[2].

For the free text questions, we have read every response and while we cannot reflect every point that was made by every respondent, we coded each response to identify themes. We have, in the summary below, provided an overview of the key or notable themes identified. We have strived to provide a balanced overview, reflecting the range of views expressed in the consultation.

THE CURRENT LANDSCAPE - THE CHALLENGES

The consultation document set out our understanding of the cyber security professional landscape based on extensive pre-consultation engagement. It noted that the cyber security profession is relatively new and has developed organically over recent years.

It went on to say that the profession is broad and varied and those working in the cyber security ecosystem are found across multiple disciplines including engineering, technology, business, social science, compliance and law, with a wide range of different competencies. We set out that there are many widely recognised cyber security roles, from technical roles like penetration testing through to more strategic and policy positions, such as Chief Information Security Officers.

The consultation set out a number of challenges facing the cyber security professional community. In summary, these were:

- 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.

[2] Due to rounding up there may be instances where the total % as set out in the summary of answers adds up to more than 100%. eg.. 49.5%+50.5% will be recorded as 50% and 51%

- 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.
- On 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.

Following that summary of government's understanding of the challenge, the first substantive question in the consultation document asked respondents:

Q1 - Are there any other challenges you perceive in the current cyber security professionalisation landscape that you feel need to be addressed?

Many respondents used the free text opportunity to endorse the government's summary of the challenges and there were a number of other key themes identified. Some respondents thought that senior leadership understanding of cyber security capability requirements and cyber security more generally was often lacking. This might lead to investment decisions in cyber security capability being misjudged or poorly informed.

Some respondents noted this was due to the challenging landscape of certifications and qualifications employers and users of cyber security resource had to navigate. Many thought that career pathways, and certification and accreditation routes, in cyber security were not clear and there was reference to the lack of clear independent oversight of them.

A number of responses noted there was a balance to be struck between boosting trust and standards in the profession while also not inadvertently preventing or dissuading new entrants from entering the profession. While the consultation did not propose it, some respondents said that cyber security was still too new and immature a domain for license to practice and regulation of cyber security professionals. Other

responses spoke about the need for a licence to practice regime.

The agility of the profession to respond to technological and other change was another key theme in the free text responses. Some respondents referenced specifically the impact that Artificial Intelligence and Internet of Things are having on the work of cyber security professionals, and the importance of professional bodies being able to respond to these developments by helping professionals keep their skills and expertise up to date.

Another strong theme was ensuring the cyber security profession has the right blend of technical and softer skills. Some respondents linked this to the diversity of the profession - both in terms of the demographics of the profession and the collective blend of skills.

Respondents also raised questions around taxonomy and definitions of cyber security. In particular, some questioned the boundaries of cyber security as a domain and where it merges in to related disciplines, such as physical security. Some respondents also noted it was unclear what defines or constitutes a cyber security professional. Some thought ‘cyber security professional’ was too broad a term for a sector that is, it was noted, made up of a series of distinct but related disciplines rather than a singular profession.

CREATION OF A NEW UK CYBER SECURITY COUNCIL

The headline proposal in the consultation was for there to be a new, independent **UK Cyber Security Council** to drive delivery against a series of objectives to develop the profession. The original consultation set out that we envisaged the Council would have organisational, rather than individual, membership and be made up of existing professional bodies and other organisations with an interest in cyber security.

The Council would aim to bring coherence to a broad range of specialisms or constituent organisations while allowing them to maintain their individual or unique offerings. We were also clear that the proposal was not about duplicating or replacing existing organisations, or expecting individuals to join an additional organisation.

To be viable and have the buy-in required, the consultation explained that the Council would need to be designed, owned and operated by the sector, with broad support from across the ecosystem it seeks to represent. We were purposely not prescriptive in the consultation document about precisely how that should be implemented, but rather set out a series of fundamental attributes and functions we believed the Council should develop and perform.

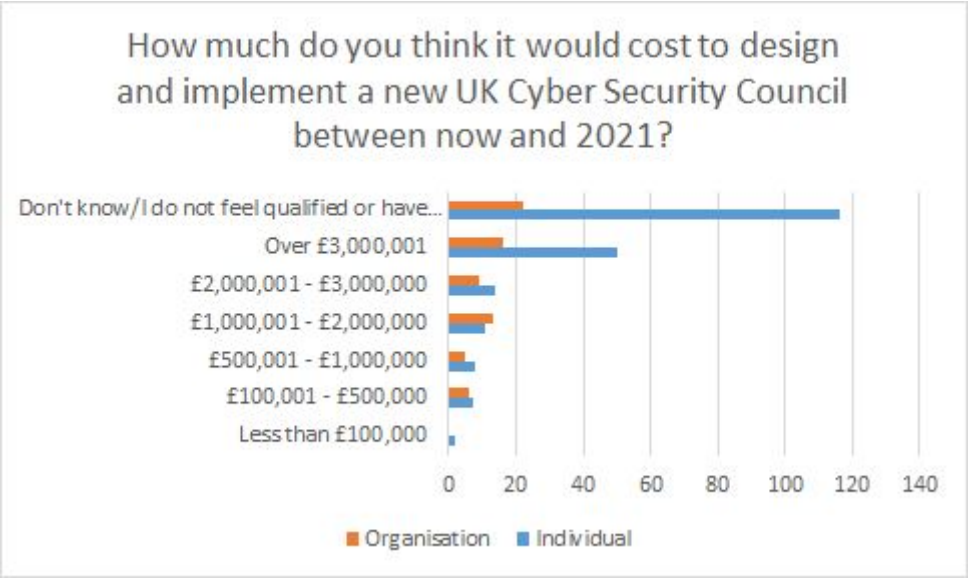
The consultation posed five questions on the Council proposal which covered its concept through to its implementation.

Q2 - Do you think that a new UK Cyber Security Council is an appropriate way of delivering on the objectives set out above in the consultation document?

Of the 282 respondents to the question, 193 (68%) thought the UK Cyber Security Council was an appropriate way of delivering on the objectives, 53 (19%) thought it wasn't and 36 (13%) respondents answered they didn't know.

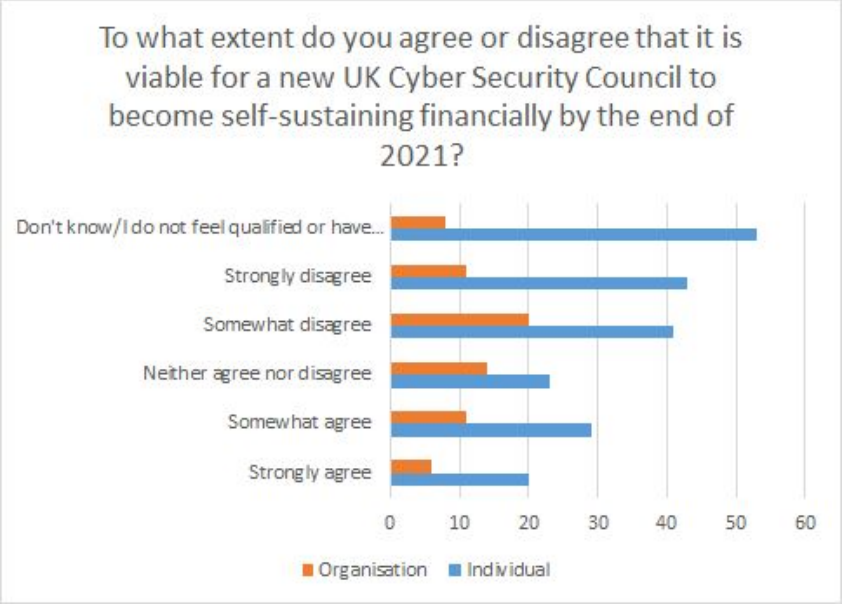
Q3 - How much do you think it would cost to design and implement the Council between now and 2021?

Almost half (140) of the 282 respondents to this questions said they did not know or did not feel qualified or had insufficient information to make an informed choice. Of the other possible answers, the largest grouping was for over £3m, which 66 (23%) of respondents selected. 23 (8%) respondents answered between £2-3m and 25 (9%) answered between £1-2m. 13 (5%) respondents selected £100,001 - £500,000 and another 13 (5%) selected £500,001-£1m. Two respondents (1%) thought it would cost less than £100,000.



Q4 - To what extent do you agree or disagree that it is viable for a new UK Cyber Security Council to become self-sustaining financially by the end of 2021?

In total 115 (41%) respondents said they either disagreed or strongly disagreed. A further 99 respondents (35%) said they neither agreed or disagreed, did not know, did not feel qualified or did not have enough information to make an informed choice. A minority of respondents, 68 (24%), said they agreed or strongly agreed that it was viable for the Council to become self-sustaining by the end of 2021.



Q5 - Why do you think that it is or is not viable for a new UK Cyber Security Council to become self-sustaining financially by the end of 2021?

This was a free text question and was asked to explore the rationale for the answers to the multiple choice questions about financial viability of the Council in more detail. When we analysed the responses, the most prominent theme to emerge related to the financial mechanism for the Council being unclear. These respondents highlighted that they thought the funding window was too short and if government funding only ran until 2021, there was a risk that the Council would fail to deliver the objectives or not be sufficiently robust to sustain itself beyond then.

An illustration of this can been seen in the quote below from an organisation who responded::

> *"Government should commit to further funding beyond 2021 to ensure that the Council achieves its key objectives. [We] would suggest that funding is staggered over a longer period of time to ensure that the organisation is viable in the long term and to give it time to develop sufficient reputation and to demonstrate its value to members. It will not become a success overnight and as such [we] feel that the timescales suggested will likely be too short to be self-sustaining in less than 3 years."*

Additionally, respondents referenced the fact that cyber security professionals were already paying membership fees to existing professional organisations so it was unclear where funding would come from. Some respondents thought more work needed to be done to establish the precise financial mechanism and standing it up should be the focus, rather than its sustainability.

A number of respondents noted the importance of the financial model not affecting the independence of the Council or its ability to act decisively in the best interests of the profession. An individual respondent said, for example:

> *"I do not think the council is a bad idea however the funding does raise a degree of concern. If the council were to be controlled and funded purely by non-government organisations then would they not direct it to their needs. If not then why would they invest their intellectual and financial resources. Perhaps as long as there are checks in place this may not be an issue."*

Another theme that emerged was how likely it was that a Council would have the capacity and maturity to deliver the range of objectives set out in the consultation in

the timescales defined. Some respondents referenced the complexity of setting the Council up and defining how its governance arrangements could impact on delivery timescales. An example of a response from an organisation on this theme was:

> *"The key attribute for a new UK Cyber Security Council is the ability to move at speed in order to address what is already a pressing issue for employers. Although we believe the objectives set out in this consultation are the correct ones we are concerned about the long timescales proposed for their delivery."*

While some respondents questioned both the government and industry commitment to the Council, responses were broadly positive about the commitment of government and industry to making this happen. One response applauded the ambition of the proposals and another noted other countries would be watching with interest to see whether the initiative was a success.

Q6 - Are there any other attributes you think would be key for the new Council to include?

We identified a range of themes in the responses to this question. A key one was the diversity and make-up of the Council. This included ensuring that it has broad representation from across the different specialisms in cyber security and represents both those with a formal education in cyber security and those with a more vocational background. We also heard it should have representation from non-cyber security professionals in related professions and sectors and must be representative in terms of ethnicity, gender, age and geographical location.

Respondents thought it would be important to have a robust mechanism/process for the selection and management of its constituent organisation members. Reflecting what we heard in the question on financial viability, a selection of respondents spoke about the need for industry and government to support the Council but at the same time, it must be independent. We heard from one individual, for example, who said:

> *"Smaller organisations provide very good insight and should have an equal voice to that of larger companies. I am concerned a council will be dominated by larger companies who have the ability to fund the council, reducing the voice of smaller researches [sic] and companies."*

Some respondents noted that it should have clearly defined relationships with organisations such as NCSC and wider government. We heard that government approval/backing was key to making the Council credible and that the Council

needed to be backed by appropriate communications and marketing. An individual respondent said, for example:

> *"A new council like this needs huge marketing in my opinion. If the whole country is aware of it (whether they are in the industry or not), then these new initiatives are so much more successful. TV, social media and radio advertising to launch it means more coverage into understanding what the government are doing. Moreover, I think the country backs trailblazing ideas like this."*

Another theme we identified was on the ability of the Council to act and help to coordinate the current bodies and organisations that exist and are offering accreditation and certification in cyber security. A number of respondents commented that it was important to avoid it becoming a talking shop and that it must have a clear value proposition for its members.

Other respondents noted that it would be important to avoid duplication with other bodies in this space. We also heard that its location should not be London focused and that it was important it was seen to represent the whole of the UK.

OBJECTIVES TO DEVELOP THE PROFESSION

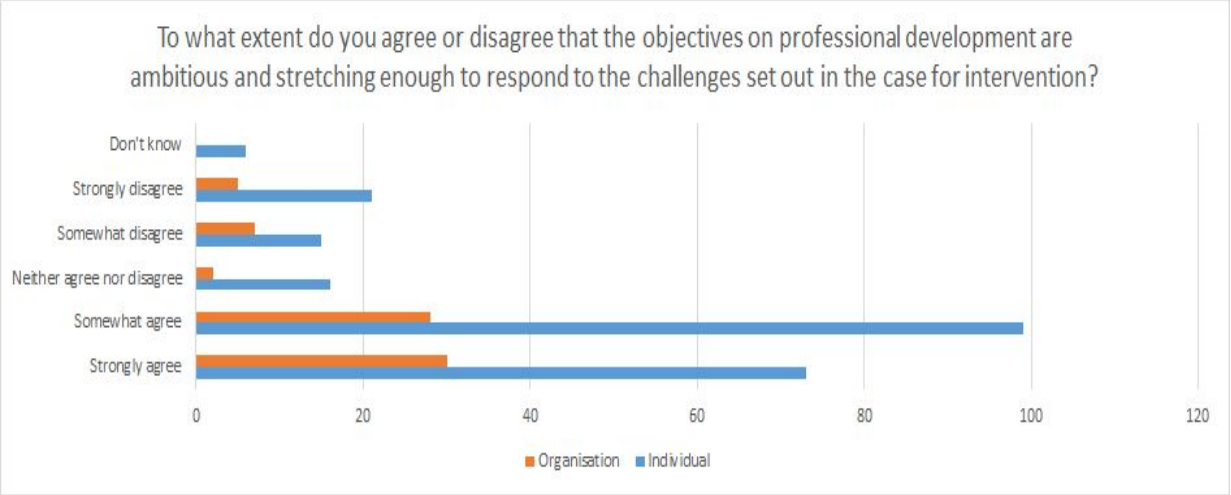
The consultation set out four broad objectives for the Council to deliver by the end of the National Cyber Security Programme window in 2021. These were focused around the themes of professional development, professional ethics, thought leadership, influence and outreach, and diversity.

Q7 - To what extent do you agree or disagree that the objectives on professional development are ambitious and stretching enough to respond to the challenges set out in the case for intervention? *Strongly agree, somewhat agree, neither agree or disagree, disagree, strongly disagree, don't know*

106 of the 305 respondents (35%) strongly agreed and a further 127 (42%) somewhat agreed with the objectives on professional development.

These objectives were specifically focused on creating a framework, agreed across the profession, which sets out the comprehensive alignment of career pathways through the profession, leading toward a nationally recognised career structure adopted by the whole cyber security sector across the UK. We went on to set out that as part of that framework, there should be full implementation of routes to chartered status for cyber security professionals across all specialisms in cyber security by 2021.

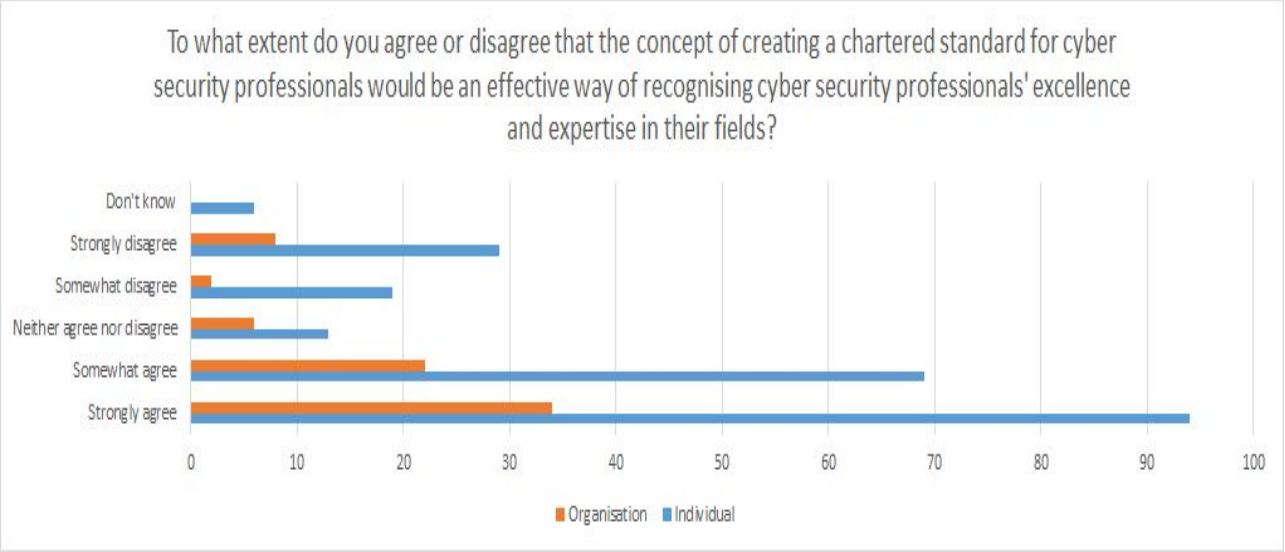
A small proportion of respondents (28 - around 9%) answered don't know or that they neither agreed or disagreed with the proposals. 26 (9%) said they somewhat disagreed and 18 (6%) said they strongly disagreed with the proposals.



Q8 -To what extent do you agree that the concept of creating a chartered standard for cyber security professionals would be an effective way of recognising cyber security professionals' excellence and expertise in their fields? *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know*

There were 305 responses to this question, which pertained to the proposal in the professional development section of the consultation which set out that we expected there would be a common Royal Chartered Status for individuals to aspire to across the range of cyber security specialisms. We set out that this should represent the gold standard of expertise, excellence and professional conduct in the profession, and be integrated into the framework of existing qualifications and certifications. We went on to say that cyber security professionals should have a clear and consistent view about how they progress towards obtaining the status.

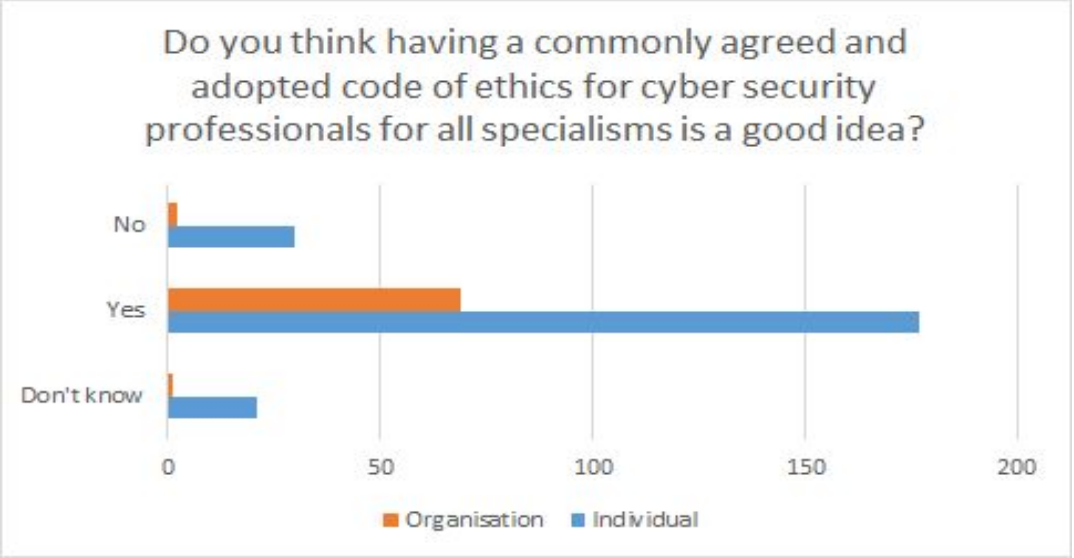
131 (43%) respondents strongly agreed and a further 91 (30%) somewhat agreed. 21 (7%) respondents said they somewhat disagreed and 37 (12%) said they strongly disagreed with the proposals. A further 25 (8%) said they didn't know or neither agreed nor disagreed with the proposals.



Q9 - Do you think having a commonly agreed and adopted Code of Ethics for cyber security professionals for all specialisms is a good idea? *Yes/No/Don't know*

We set out that a key objective for the profession should be the production of draft Code of Ethics, agreed voluntarily between participating cyber security professional organisations, which is applicable across the whole of the cyber security sector. The consultation document set out that the Code of Ethics would be one of the foundation stones to ensure individuals have a clear framework and guiding principles to exercise professional judgement. It would enable organisations and individuals to share their experience in order to achieve a clearer overview of good ethical practice and to reduce exposure to risk in this area.

This proposal was very strongly supported in the responses. 249 (82%) of the 303 responses answered yes to the question of whether it was a good idea with 32 (11%) answering no to the question, and a further 22 (7%) saying they didn't know.



Q10 - Why do you think it is or is not a good idea to have a commonly agreed and adopted Code of Ethics for cyber security professionals of all specialisms?

The next question gave respondents an opportunity to set out their views in more detail on the proposed Code of Ethics. There was a strong theme of endorsement of the proposal in the free text answers - with over half of those who took the opportunity to respond restating they thought it was a good idea. Some respondents thought it would bring more coherence to the existing landscape, recognising that there were similar codes or frameworks in existing professional organisations. There were suggestions about what it might cover, with a number of respondents identifying whistleblowing as a specific area it should address.

An example of a broadly supportive response was:

> *"It is vital that all professionals carrying the Chartered designation are trusted. The very nature of the work conducted by Cyber Security practitioners/ professionals will give them access to the most sensitive information and intellectual property of the client organisation. It is imperative that such practitioners/ professionals are bound by strict codes of ethics and are thereby both accountable and answerable for their actions."*

We also identified themes around the importance of having a robust mechanism to monitor and where appropriate enforce the Code. Some respondents commented that without this it would not be as effective. While other respondents thought that cyber security was too broad a domain to have a singular Code of Ethics and that it could conflict or duplicate existing Codes or frameworks. Below is an example

response on that theme:

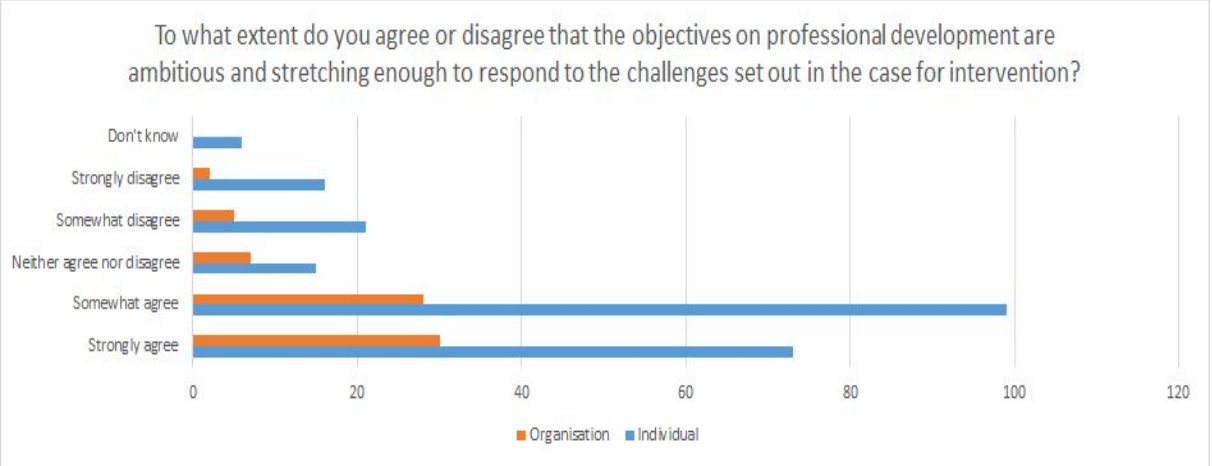
> *"It's [cyber security] a very broad area that I think will be too difficult to create an ethics code for all specialisms. It [sic] think we'll end up with something so broad it'll be useless. Some areas such as professional services firms have their own ethics requirements as do those with law degrees which may conflict".*

Q11- To what extent do you agree or disagree that the objectives on thought leadership are ambitious enough to respond to the challenges set out in the case for intervention? *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know.*

The deliverables on thought leadership and influence set out in the consultation were focused around the appetite for strong and visible leadership to coordinate the views of and speak authoritatively on behalf of all of the different specialisms and organisations in cyber security. We set out that this is crucial not only for speaking coherently to the different parts of the cyber security ecosystem, including government, but also, given the importance of cyber security to all sectors of the UK economy, for more effective reaching out to and development of links with other sectors.

We went on to define a series of deliverables between now and 2021, such as there being an agreed strategy, developed across the profession, to define and strengthen relationships with other professional sectors with interests in cyber security such as law and insurance.

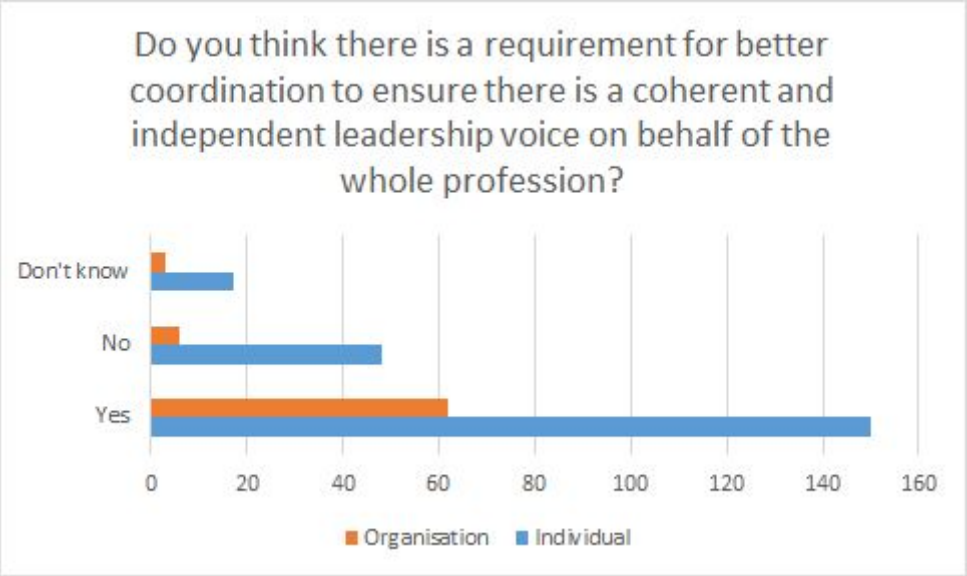
The responses show strong support for the proposals on thought leadership and influence. 94 (33%) of the 287 respondents strongly agreed and a further 116 (40%) somewhat agreed that the objectives were stretching enough to respond to the challenges set out in the case for intervention. 21 (7%) somewhat disagreed and 20 (7%) strongly disagreed, with the remaining 36 (12%) answering that they didn't know or neither agreed nor disagreed with the proposals.



Q12 - Do you think there is a requirement for better coordination to ensure there is a coherent and independent leadership voice on behalf of the whole profession? *Yes/No/Don't know*

As part of the thought leadership and influence question, we also set out that during 2019 we expected an agreed and adopted vision statement and roadmap for how the profession as a whole will provide coordinated leadership and influence other sectors and government in the best interests of the profession. This reflected the view set out in the case for intervention that our pre-consultation engagement showed there to be an appetite for strong and visible leadership to coordinate the views of and speak authoritatively on behalf of all of the different specialisms and organisations in cyber security.

Of the 289 respondents, 215 (74%) answered 'yes' to the question on whether there is a requirement for better coordination to ensure there is a coherent and independent leadership voice on behalf of the profession. 54 (19%) respondents answered 'no' and 20 (7%) said they didn't know.



Q13 - Are there any other policy or professional development issues where you think the profession should lead on the development of an agreed position?

In the thought leadership and influence section of the consultation, we set out that there should be coordinated thinking and proposals on behalf of the different specialisms within the profession to further strengthen it. This could include on issues such as regulation of cyber security professionals and a licence to practise for example. It is worthwhile restating that we are not proposing a licence to practice regime but rather the profession should have a coordinated view on issues relating to the profession.

This question asked whether there are other policy or professional development issues where the profession should lead on the development of an agreed position. There was a wide range of responses to this question. The most commonly raised themes were:

- Boosting the visibility and understanding of the profession and cyber security as an issue amongst senior leaders, other professions/industries and the general public
- Diversity within the profession. There were specific issues raised like supporting more neurodiverse candidates in to the profession and increasing the number of women, as well as more generally boosting the blend of skills and capabilities in the profession. This includes non-traditional routes in to careers in cyber security.
- International alignment and ensuring the UK is well placed in what is a global industry

- Advocating and promoting standards (ISO etc.) and quality assurance, risk management and assessment guidance and support

We also heard that in working together and developing coordinated responses to policy challenges that the cyber security professional community still needs to be able to embrace its diversity of thought and range of different specialisms. One respondent (an organisation) said:

> *"I agree with the goal of providing 'coordinated and visible thought leadership; however, we must be very careful here to avoid the quieting of dissenting and confusing opinion with fact. Also, there is the very real danger of a concentration of commercial interests acting to exclude each other from participation. Coordinated and visible thought leadership is absolutely essential; however, this must be a place where we leave our corporate hats at the door and come together as stewards of the profession with the understanding that we are acting in the best interests of the profession and society as whole".*

Q14 - To what extent do you agree or disagree that there is a requirement to produce a clear mission statement, agreed across the whole cyber security profession, on how the profession will develop the next generation of cyber security professionals? *Strongly agree, agree, neither agree or disagree, disagree, strongly disagree, don't know.*

We set out in the consultation that cyber security needed to be seen as an attractive and viable career option for a greater, more diverse range of people. We recognised the progress made thus far, but noted that we thought more coordination was required to reach out to and develop the next generation of cyber security professionals. We set out a series of deliverables relating to this, framed around the development of a clear mission statement, agreed across the whole cyber security profession on how the profession will develop the next generation.

We asked if respondents agreed there was a requirement to do that. 155 (54%) of the 289 respondents strongly agreed there was, with a further 69 (24%) somewhat agreeing. 19 (7%) somewhat disagreed and 23 (8%) strongly disagreed. The remaining 23 (8%) neither agreed or disagreed, or answered 'don't know'.


To what extent do you agree or disagree that there is a requirement to produce a clear mission statement, agreed across the whole cyber security profession, on how the profession will develop the next generation of cyber security professionals?
Somewhat disagree
Strongly disagree
Strongly agree
0
20
40
60
80
100
120
Organisation
Individual

CONCLUSIONS - IMPLEMENTING THE OUTCOMES OF THE CONSULTATION

Overview

The consultation purposely took place at an early stage in policy development to ensure anyone with an interest in the development of the cyber security profession in the UK could meaningfully contribute. We are extremely grateful for the level of engagement and interest in the consultation, and the depth, expertise and insight shown in the responses.

We believe this provides us with a robust basis on which to draw informed conclusions about next steps and the future direction of the proposals. This section sets out our conclusions, explaining either where we propose to amend or slightly adjust proposals based on consultation evidence and where we intend to proceed without amendment.

Overarching conclusion

We believe the responses to the consultation represent strong support for the main thrust of the proposals; which is to define a series of objectives and to create a new UK Cyber Security Council to coordinate delivery. Given the level of support, we do not believe there is reason to revisit the fundamentals of those proposals and intend to proceed to identify a lead for the design and delivery of the UK Cyber Security Council. This will be done through a grant funding competition which is being issued in parallel with this government response.

The responses to the consultation helped significantly refine and finesse our thinking and add an extra layer of granularity to our proposals. This has shaped core criteria against which applications for funding will be assessed. One of the key areas is around implementation and delivery of the Council. There were reservations about the extent to which the ambition for the Council can be delivered in the timescales and in a way that ensures the Council is financially self-sustaining beyond 2021. We have addressed this, and other issues such as prioritisation of objectives and reservations around chartered status for cyber security professionals, in the section below. This is reflected in the core criteria for the grant funding competition set out at **Annex 1.**

Financial model and sustainability of the Council

The consultation document set out an ambition for the Council to become self-sustaining beyond the government funding window (mid-2021). Our rationale

was that the Council would bring significant benefits to the profession and there was significant scope to design and shape the Council.

We believe the ambition for the Council to become self-sustaining is still the right one but recognise, based on the feedback from the consultation, this could be challenging in view of the ambitious objectives and timescales. We also recognise there is a need to set out, in more detail, how government anticipates the Council developing a sustainable financial model in its design and embryonic stages.

The associated funding competition explains that we will make available funding of between £1m to £2.5m over the remainder of the National Cyber Security Programme to design and deliver the Council. We believe that a government contribution within this range, over two years, combined with other sources of funding, is sufficient to cover the design and set-up costs of the Council, and deliver the prioritised objectives which are set out below.

This may cover areas such as initial staff and consultancy costs to draft and agree governance provisions, running and administration costs and early marketing and communications spend. It would also, we believe, allow for the Council to start delivering the prioritised objectives around professional development and developing an agreed Code of Ethics.

The government contribution would represent seed-funding and would be issued as a grant contingent on delivery against agreed milestones. To agree the milestones we would expect the delivery lead to produce a clear business case for spend of that government funding and a clear roadmap for how the Council intended to explore financial sustainability. By way of example only, we might expect the Council to work with constituent organisations to explore whether some form of levy system could make a contribution, both financial and in-kind, to the running of the Council.

We would also expect the Council to identify areas of potential revenue generation which do not compete with its constituent organisations. For example, we would expect the delivery lead to develop a detailed financial model for Chartered Status. We know this can be a key revenue generator for other professions.

The original consultation document set out that while the NCSP comes to an end in 2021 and future funding cannot be guaranteed, government will continue to support the resulting mechanism and remains committed to the long term delivery of the overarching strategic outcome. This remains true, and government will work with the delivery lead to determine the extent and nature of government support to the Council beyond 2021. In parallel, government would expect to work closely with the

Council delivery lead to, where appropriate, use government levers to help identify means of sustaining the Council beyond 2021.

To ensure the viability of the Council beyond 2021 in a range of scenarios, we would expect the delivery lead to work with government to develop robust plans for the possible scenarios beyond the guaranteed government funding window. This would explore approaches to a scenario where there was no further government funding beyond March 2021, government funding of less than £200,000 per year for a period of 3 to 5 years beyond March 2021, and a level of government funding roughly similar to the grant being applied for and lasting for three to five years beyond March 2021.

A Clear Value Proposition

While there was strong support for the Council as an appropriate mechanism to coordinate delivery of the objectives set out in the consultation, a number of respondents questioned why any organisation or individual might want to be part of the Council. We believe this is an important point to address. The Council's financial model can only be robust if the Council has a very clear value proposition for its constituent members and the cyber security community in the UK.

The consultation articulated government's view on the overarching benefits of the Council model. It set out that a new mechanism could bring more coherence, coordination and consistency at a national level, and across the whole cyber security profession, in pursuit of common objectives. This, we believe, would ensure that the wide range of existing activity to develop the profession would be more effective. The Council, in coordinating activity and providing a focal point, could help drive progress more quickly on, for example, the flow of new talent in to the profession and the challenges individuals and employers have in understanding the cyber capability they have and need.

However, we recognise there needs to be a clear articulation of the direct benefits for organisations in joining the Council. This benefit also needs to be clear to the individual members of those prospective organisational Council members. It is not reasonable to expect this to be an altruistic endeavour. We have sought to articulate these benefits below:

- First, we believe the Council would help boost the profile of its constituent members and by acting as the front door in to the profession, help to more effectively direct individuals and organisations to the most appropriate existing professional organisation.

- Chartered status - being able to work towards something that is seen as a gold standard would be attractive. This may provide the ability to drive revenue and attract new members.
- Access to part of the government seed-funding to develop existing initiatives to deliver objectives set out in this document.
- In its outreach activity, we would expect the Council to materially help organisations promote their offerings by leveraging the collective networks of its other constituent members.
- Greater influence over policy makers and related professions and disciplines. We would also expect the Council, as the focal point for the profession, to be able to effectively lobby and influence other professions, the wider cyber ecosystem and government in the interests of its constituent members.
- Benefits of being part of a more cohesive community of organisations who have common and agreed objectives to develop the profession. This will include facilitating better international collaboration and relationships, better access to international markets and sharing of best practice.
- Being involved in a new and ambitious initiative that has been supported by a public consultation and has broad backing from across the cyber security community. It is also an opportunity to help design it rather than it be enforced or retrofitted.

Ability to act and appropriate representation

As set out above, the support for the Council model was caveated by some respondents who spoke about the importance of its ability to take action and be agile enough to respond to emerging challenges and changes affecting the profession. We believe fundamentally that the Council needs to be able to act, and needs to have the ability to work with its constituent organisational members to respond quickly to emerging challenges.

Central to this will be having strong governance and a strong constitution. We recognise that a range of different organisations may be involved in the Council – ranging from charities, to not for profit organisations, to academic institutions and a range of businesses and commercial enterprises. We would expect the delivery partner of the Council to quickly develop interim arrangements for the design phase of the Council, with a clear roadmap to developing robust and enforceable governance arrangements for constituent members.

The composition of the Council is also central to it being able to act with authority and have the credibility it needs both within the cyber security community and beyond. We heard in the consultation that the Council needs to have appropriate representation from across the cyber security community to ensure it can effectively

serve the interests of the broad range of interested groups and individuals. This includes existing professional organisations, academia, cyber security businesses and employers and government. We also heard clearly that the Council would need to have non-executive directors, or equivalent, to hold it to account on delivery and independence. It may also have experts from other professions and disciplines to strengthen its external links and representation which covers all parts of the UK, including devolved administrations. It would also need to work closely with the National Cyber Security Centre to ensure it had a well defined relationship with the UK's technical authority for cyber security.

We believe getting representation right is crucial to the Council being an effective, credible and collaborative endeavour. We want to reiterate that the Council should not seek to replicate or replace existing professional organisations and should seek to define its role as not being in competition to other related Councils or umbrella organisations.

Prioritisation of Objectives

While there was broad support for the deliverables set out in the consultation, we recognise the level of ambition was high and we need to set out a realistic expectation on what can be delivered. We accept that the design of the Council will be a complex process, which may involve detailed discussions between a variety of different organisations, many of whom have different legal statuses and memberships to discuss the proposals with. We also believe that spending time at the outset to develop a robust business plan, operating model and roadmap is key to ensuring the Council is sustainable in the longer term.

We have therefore reviewed the deliverables set out under each objective in the consultation to refine and prioritise them. We have considered this in light of what we heard in response to the questions in the consultation on the challenges facing the cyber security professional community and our assessment of where focus is needed most urgently.

We believe that the deliverables in the **professional development objective** represent the most pressing area for progress. This is at the root of the challenge cyber security professionals have in articulating their capabilities in a way that a broad range of potential employers or users of their services can understand, and for organisations trying to determine what capability they need to recruit or contract.

We consider that while many of the existing qualifications and certifications are valued by individuals and employers, there is a clear requirement for a UK framework to help individuals and organisations navigate the landscape and make informed

decisions. This framework is a crucial foundation for the delivery of the commitment set out in the 2016 Strategy for the profession to achieve Royal Chartered Status by 2020.

The deliverables on professional development and the Code of Ethics therefore remain broadly unchanged, but we have acknowledged in the timescales the initial work that will be required to set up the Council. We have also defined in more depth the outcomes we would expect to see in the design and embryonic stages of the Council:

By end of 2019:

- Agreed governance approach and legal status resolved.
- Agreed approach to communications and marketing of the Council to articulate its role and how it relates to its constituent organisations and the rest of the cyber security professional landscape.
- A clear business plan and roadmap for delivery of prioritised deliverables.

By March 2020:

- The early development and alignment of a coherent set of career specialism pathways, both into and through the cyber security profession, clearly identifiable and widely agreed across the cyber security sector and with government. This should include the alignment and coordination of the vast range of valuable professional qualifications and certifications which span both vocational and academic certification already available. It should also allow for inclusion of future qualifications that may be introduced to support legislation and technological advancement.

- A draft Code of Ethics, agreed voluntarily between participating cyber security professional organisations, which is applicable across the whole of the cyber security sector.

By end of 2020:

- Developed proposals for, and early implementation of, a common Royal Chartered Status for individuals to aspire to across the range of cyber security specialisms. This should represent the gold standard of expertise, excellence and professional conduct in the profession, and be integrated into the framework of existing qualifications and certifications. Cyber security professionals should have a clear and consistent view about how they progress towards obtaining the status.

- Clear proposals for how the Code of Ethics would be applied and enforced fairly, robustly and consistently across signatory organisations.

By March 2021:

- A framework, agreed across the profession, setting out the comprehensive alignment of career pathways through the profession, leading towards a nationally recognised career structure adopted by the whole UK cyber security sector.

- As part of that framework, full implementation of routes to Chartered Status for cyber security professionals across all specialisms in cyber security.

- Full implementation and application of the Code of Ethics with signatory organisations

A new Profession Comprised of Different Specialisms

Many respondents felt uncomfortable with the term ‘cyber security profession’ and we heard from a number that cyber security was a broad domain with distinct but related specialisms. We noted in the original consultation that cyber security is still a relatively new domain which has developed quickly and organically over recent years. This means the parameters of cyber security and the taxonomy and definitions used by those engaging are not as well defined, or widely agreed, as in other sectors.

We believe this is important to address because, as much as is possible in a fast changing and relatively new domain, we want those involved in it and related to it to have a clear understanding of what we mean when we talk about a profession for cyber security.

The National Cyber Security Programme has undertaken a project to define the foundational knowledge upon which the field of cyber security is built. The Development of the Cyber Security Body of Knowledge (CyBOK) project is being undertaken by a team of UK academics, led by Bristol University, in consultation with the national and international cyber security sector. Phase One, completed in October 2017, focussed on defining the scope of cyber security. The resultant 19 Knowledge Areas are now being developed in further collaboration with the sector and academia.

We believe the CyBOK should be the starting point for the Council in defining its remit and parameters as it defines a scope for cyber security agreed by the national

and international cyber security community as well as the knowledge required to practise across the breadth and depth of the cyber security domain.

Chartered Status for Cyber Security Professionals

We set out in the consultation that we expect the Council to oversee the development of a Royal Chartered status as the gold standard of expertise, excellence and professional conduct for cyber security professionals to aspire to. While supported by the majority of respondents, we noted the concerns from a minority of respondents about the concept of a Chartered Status and wanted to clarify a number of points about how we envisage it being implemented:

- We envisage the Council licensing its organisational members to offer a common Chartered Status to their individual members.
- That would allow the range of organisations, some of whom may separately have been incorporated by Royal Charter and others who have not, to issue a common Chartered Status for cyber security overseen by the Council.
- There are a number of possible ways to implement this objective. One option would be for the Council to create a proposal for and apply for a completely new chartered standard. Alternatively, an existing chartered status of a constituent organisation of the Council could be slightly modified or amended. Each of these options would be subject to approval by the Privy Council but we would expect the UK Cyber Security Council to work with its constituent members to develop workable and viable proposals to deliver on this objective. Government is open minded about precisely how it is delivered.

NEXT STEPS

As set out above, this response is being issued in parallel with an invitation to apply for government funding to lead the design and delivery of the UK Cyber Security Council. This is being issued as a competitive process. All proposals will be evaluated against published core criteria and requirements, and an assessment made to select one successful proposal.

The original consultation document set out that if we did proceed to this stage, it was likely proposals would need to show they can command broad support across the cyber security professional development landscape and wider cyber ecosystem. We believe the outcomes of the consultation endorse that and this remains the key principle for the funding competition. We recognise a competitive process, of any sort, may lead to challenges in the existing community and the criteria set out below therefore places significant emphasis on being able to command support across the cyber community.

Alongside that, the evidence received through the consultation and the conclusions set out above have informed the development of core criteria against which proposals will be assessed. So where, for example, we concluded that we needed to prioritise deliverables, there is now a corresponding criterion about producing a clear and agreed roadmap for delivery. We have also built in strong criteria around financial viability in a range of scenarios. The core criteria for proposals are at **Annex 1.**

The full competition criteria and applicant guidance are being published alongside this government response. The application window will be open from 21 December 2018 and closing at 16:00 on 28 February 2019. DCMS and the National Cyber Security Centre will hold briefing sessions for prospective applicants in January. Please email csprofession@culture.gov.uk if you would like to register your interest in attending one of the briefing sessions.

Following the closure of the bidding window on 28 February 2019, government will assess proposals and conduct due diligence, with a view to identifying and announcing the successful proposal by April 2019.

ANNEX 1 - CORE CRITERIA FOR PROPOSALS

Every application will be expected to evidence that it meets the following eight core criteria:

OVERALL FIT AND VISION FOR UK CYBER SECURITY COUNCIL

1. Has a strong and comprehensive understanding of the cyber security landscape and the challenges and opportunities for cyber security professionals in the UK

2. Shows clearly how the UK Cyber Security Council will have as full and broad representation as possible from across the cyber security community together with the right blend and level of expertise to ensure the UK Cyber Security Council is credible, sustainable and can drive excellence in the profession

3. Has a clear and viable vision for the design and structure of the UK Cyber Security Council.

DELIVERY

4. Has a clear and viable delivery plan and roadmap, with clear timescales for each stage, for the design and maturity of the UK Cyber Security Council - from its inception to mid-2021.

5. Sets out a clear delivery plan to deliver the prioritised objectives associated with Professional Development, Code of Ethics, Thought Leadership and Outreach. The indicative prioritised set of delivery milestones is set out at section 8 of Annex A (Application Process and Guidance for Applicants) of the Request for Proposals.

6. Has the capability, expertise and a proven track record in delivering similar and comparable projects to time, budget and quality.

FINANCIAL PLAN, GOVERNANCE AND RISK MANAGEMENT

7. Has a credible, viable and appropriate approach to conflict resolution, governance and risk management.

8. Has a robust and appropriate financial plan to ensure public funds are used in a way that gets the best value for money. The financial plan

should also set out clearly the approach to ensuring the Council is sustainable financially in the following scenarios over its first 5 years:

(a) no further government funding beyond March 2021
(b) government funding of less than £200,000 per year for a period of 3 to 5 years beyond March 2021
(c) a level of government funding roughly similar to the grant being applied for and lasting for 3 to 5 years beyond March 2021

Specifically, the plan must set out how the new UK Cyber Security Council would explore and identify additional means of funding and income generation both during and beyond the period of the government grant.

There will be additional prerequisite conditions any applicant will have to meet. These are defined as Gateway Questions in the grant competition guidance and application forms. For example, proposals must bid for an amount of funding within the parameters defined and proposals must be signed off by a Chief Executive Officer or equivalent.