Department for Digital, Culture, Media & Sport

REQUEST FOR PROPOSALS - A NEW UK CYBER SECURITY COUNCIL

ANNEX A - APPLICATION PROCESS AND GUIDANCE FOR APPLICANTS

Application window opens: 21 December 2018
Deadline for Applications: 16:00 on 28 February 2019

CONTENTS

1 - Introduction

The Department for Digital, Culture, Media and Sport (DCMS, hereinafter called 'the Authority') is seeking proposals for grant funding to design and deliver a new, independent UK Cyber Security Council.

This grant competition follows a public consultation issued by Government in summer 2018 which set out proposals to develop the cyber security profession in the UK, including the creation of a new UK Cyber Security Council. The competition is being issued in parallel to, and should be read alongside, the government response to the consultation on developing the cyber security profession in the UK.[1]

As set out in the government response, the consultation showed strong support for the Council model. There was also strong support for the objectives and deliverables it was anticipated the Council would coordinate delivery on. This included developing a Code of Ethics which is adopted across the cyber security profession and developing a common Royal Chartered status for cyber security professionals to aspire to as the gold standard of trust and expertise.

The response to the consultation sets out that in view of the level of support shown, Government will proceed to identify a delivery lead to design and deliver the new UK Cyber Security Council. This document sets out the process the Authority will follow, including the criteria that will be applied when assessing applications and the funding available.

Government is initially committing to making available between £1,000,000 to £2,500,000 funding from the National Cyber Security Programme over financial years 2019-2020 and 2020-2021. We believe that a government contribution within this range, over two financial years, combined with other sources of funding we expect the delivery lead to identify and secure, is sufficient to cover the design and set-up costs of the Council, and to deliver the prioritised objectives which are set out in the government response to consultation.

The core criteria against which applications will be assessed are set out in section 3 below, alongside associated confidence indicators. We recognise a competitive process, of any sort, may lead to challenges in the existing community. The original consultation document was clear that it was likely proposals would need to show they can command broad support from across the cyber security professional development landscape and wider cyber ecosystem. The criteria for assessing Applications therefore places significant emphasis on how Applicants intend to

[1] https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession

generate the support from the cyber security community and bring the existing landscape of professional organisations together in a more coherent way.

The grant competition will be run by DCMS and supported by other government departments and agencies, including the National Cyber Security Centre (NCSC). Applicants should note that this is a grant competition rather than a tender for contracts but the process will follow a similar format. We anticipate identifying one successful applicant - that applicant may be a single bidder or a consortium. We envisage the legislative authority for the grant will be section 8 of the Industrial Development Act 1982.[2] We anticipate the work to design the Cyber Security Council commencing in April 2019.

This guidance document constitutes the Conditions of Application Process and guidance for the Request for Proposals (RFP). Participation in the application process automatically signals that Applicants accept these Conditions. All references to 'the Authority' throughout these documents refer to the Department for Digital Culture Media and Sport (represented by the Secretary of State for Digital, Culture, Media and Sport). The required structure and content of Applications are detailed in Annex B: 'Grant Competition Application Form'.

These instructions are designed to ensure that all Applications are given equal and fair consideration. It is important therefore that you provide all the information requested in the format and order specified. Applicants should read these instructions carefully before completing the Application documentation. Failure to adhere to these instructions may result in the rejection of the Application. Applicants are advised therefore to acquaint themselves fully with the extent and nature of the services and contractual obligations.

All material issued in connection with this RFP shall remain the property of the Authority and shall be used for the purpose of this RFP exercise. Applicants are solely responsible for the costs they incur in the preparation of any Application.

[2] https://www.legislation.gov.uk/ukpga/1982/52/section/8

2 - Application reference documents

The application process comprises the following documents which are available on the consultation gov.uk page[3]:

- Government consultation issued 19 July 2018 - Implementing the National Cyber Security Strategy – Developing the Cyber Security Profession in the UK.
- Government response to consultation on Developing the Cyber Security Profession in the UK - issued 21 December 2018
- Request for proposals to design and deliver a new UK Cyber Security Council for the UK. Annex A: Application Process and Guidance for Applicants
- Request for proposals to design and deliver a new UK Cyber Security Council for the UK. Annex B: Application Form

3 - Application Process and criteria

The application process consists of five steps: application, pre-assessment/initial due diligence, main assessment, approval/remaining due diligence and award of grant. The initial application window is open from 21 December 2018 until 17:00 on 28 February 2019. The Authority reserves the right to not consider applications submitted outside of this time-frame.

Prior to Applications being substantively assessed, they will be considered against a number of gateway questions to ensure they meet basic application requirements. Any applications that do not meet all of these requirements will not progress to the next stage of consideration. Gateway questions seek to establish:

- Application eligibility
- The amount of funding sought is within the range set out and the activities to achieve output are clearly set out.
- All organisations in an Application have or are in the process of obtaining Cyber Essentials certification.
- An Application must provide the name of the organisation and that of the individual who is submitting the Application and who will act as the overall point of contact.
- Each organisation in an Application must be listed and must provide a signed letter of support from its CEO (or equivalent) confirming that the organisation is part of the Application and has registered offices in the UK.
- The application form has been completed correctly in a clear and concise manner and word limits have not been exceeded

[3] https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession

Applications that successfully meet all the prerequisites of the pre-assessment phase will be assessed substantively against the Applicant's overall vision for the UK Cyber Security Council and eight core criteria. The eight core criteria are grouped into three core themes:

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 here at section 8.

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.

The Applicant's overall vision for the Council and each of the eight core criteria will be afforded the same weighting. The Authority will assess and score each individual criterion based on a scale 0 -10, with 0 representing 'no confidence' and 10 representing 'full and excellent confidence'.

The full assessment framework is set out in table 1 below and for each core criterion, the application form at Annex B defines a series of confidence indicators which will be used during Assessment to determine the level of confidence in the Application. It should be noted, however, that the confidence indicators listed in the application form do not constitute an exhaustive list of factors to be considered when assessing overall confidence in proposals.

Please note that where there is found to be negligible or no confidence, or little confidence (which would be any criterion scoring between 0 - 3.9 at any stage of assessment), the application will automatically be considered unsuccessful.

TABLE 1	
Scoring Interval	**Definition**
0.0 to 1.9	An Assessor reasonably has negligible or no confidence that an Application meets the required criteria for this scored section of the proposal. There are major weaknesses and deficiencies throughout this scored section.
2.0 to 3.9	An Assessor reasonably has little confidence an Application meets the required criteria for this scored section of the Application. Some of the criteria are met but it is clear that some criteria have not been met.
4.0 to 5.9	An Assessor can reasonably have some confidence that an Application meets the required criteria for this scored section of

	the Application. Most of the criteria are met but there are minor deficiencies in how the Application addresses the remaining criteria.
6.0 to 7.9	An Assessor can reasonably have good confidence that an Application meets the required criteria for this scored section of the Application. All of the criteria are satisfactorily covered.
8.0 to 10.0	An Assessor can reasonably have full and excellent confidence that an Application meets the required criteria for this scored section of the Application. The Application provides full and clear evidence that it meets or exceeds the requirement.

As part of the assessment process, the Authority may ask you to clarify any point in the Application Form. Please ensure that you provide a day to day contact for your mentioned primary contacts and that they are available for to respond to clarification questions within two days.

4 - The Assessment Process

Applications that satisfy the gateway questions will be assessed substantively against the full criteria set out above by an Assessment Panel. The panel will include representatives from DCMS, NCSC and wider government. There may also be independent and impartial representation from industry and academic experts. Each application will be read and scored independently by a minimum of three members of the Assessment Panel.

The Assessment Panel may request clarifications in writing regarding an Application before reaching a final consensus score. At the Assessment Panel's discretion, the assessment process may also include a panel interview to explore elements of the Application in more detail. The assessment may take account of any discussions the Authority has with Applicants after the deadline for submitting responses, to clarify responses and references that have been obtained.

The Assessment Panel will agree a consensus score for each scored section of each application. The Assessment Panel will determine the overall final score of each Application and produce a ranked list of applications. Where required, the Authority reserves the right to refer all comparator final scores to a maximum of two (rounded) decimal places. The Authority reserves the right to alter the timings of any of the assessment stages or to withdraw the RFP and any of the assessment stages at any time.

5 - Applicant eligibility

Applicants who seek to receive the Grant from DCMS must be either:

- A single entity which will deliver all of the Funded Activities; or
- A consortium formed from a number of organisations with shared objectives and agreed arrangements for leadership and governance. Please note that DCMS is unable to award a grant to multiple organisations. As such, the lead applicant would be responsible for distributing funding and managing working relations with other partners. The lead applicant is the responsible body who will countersign the application form and ensure the terms and conditions of the grant offer are upheld by all parties involved. It is expected that partnership agreements are already in place, or that the lead applicant has correspondence from authorised representatives at each partner organisation that confirms involvement in the project and acknowledges submission of the lead applicant's application.

Applications from the following entities will not be considered:

- Individuals
- Government departments or other public bodies
- Organisations excluded under s.8 of the Industrial Development Act 1982

6 - Funding

The range of funding being made available by Government is between £1,000,000 and £2,500,000 over financial years 2019-20 and 2020-21. We would envisage this would be evenly split between both financial years - with between £500,000 - £1,250,000 available in FY19/20 and the same range available in FY20/21.

The Authority will allocate funding to the Application that has the highest score after having been assessed against all the assessment criteria. The Authority reserves the right to apply its discretion on the amount of funding that is to be awarded to the successful Applicant. This may be in full in accordance with the Applicant's proposal. However, if the Authority deems that only part of the proposal is acceptable, in terms of the stated deliverables, then it reserves the right to award partial funding on that basis.

We envisage the total Grant awarded will be paid in eight instalments, with four instalments being paid in year one (2019-20) and four instalments in year two (2020-21). The Grant will be made on the basis that it does not constitute State Aid for the purpose of the State Aid Rules. Applicants are responsible for ensuring that their Application can be delivered in line with State Aid criteria upon which the

funding is to be awarded. Further information on State Aid is available at the following link: https://www.gov.uk/guidance/state-aid

7 - Duration of the Grant Agreement

The Grant will be awarded for the period up to 31 March 2021, to include set up and delivery of the UK Cyber Security Council. It is a requirement that funding is utilised before the 31 March 2021 and there is a presumption that funding will be paid in arrears.

Payments will be made evenly or according to the agreed milestones and deliverables (whichever deemed appropriate by the Authority) in the financial years 2019-2020 and 2020-21 up to 31 March 2021. The standard DCSM grant terms and conditions are provided at Annex 1 of the application form (Annex B). We reserve the right to vary and tailor the terms and conditions in advance of signature but wanted to provide prospective Applicants with early sight of the standard terms of the likely Grant Agreement.

Prospective Applicants are welcome to submit questions or points of clarification to DCMS on the standard grant conditions prior to submitting the application but there will be a period, after award of the grant, to agree and negotiate the specific terms.

8 - Indicative Milestones and Deliverables

Given the importance of the role of the Council to the UK cyber security community, and the level of government funding being committed, there will be a strong focus on monitoring and assurance of delivery against the grant agreement. The UK Cyber Security Council will be entirely independent of government but for the duration of the government funding window, government will maintain a strong focus on monitoring and assurance to ensure public funds are being spent in a way that maximises the impact of the funding and provides best value for money.

It is expected that Applications will set out proposals for robust monitoring of delivery. Government and the delivery lead will work together to define an appropriate governance framework for the period of government funding. It is expected this would involve at least a quarterly board meeting held with the Authority. The Authority would appoint a Senior Responsible Officer (SRO) to chair the board and board meetings would be used to review deliverables and progress towards achieving milestones.

To support the SRO, the Authority will support the grant recipient's delivery of the work where appropriate. The Authority's team is likely to comprise a policy lead, project manager and technical advisor(s).

The application process is designed to give applicants the opportunity to set out in detail their approach to delivering against the core criteria and to set out a clear, credible and robust delivery plan. As a starting point, government has defined a series of indicative milestones and deliverables below in tables 2 and 3 which set out minimum expectations. Applicants should use these, and the full government response to the consultation, as a basis for their delivery plan and refine and amend where they deem appropriate.

TABLE 2		
Milestone	**Date**	**Description**
M1	May 2019	Kick-off project meeting
M2	30 June 2019	To include: ● outline of approach to achieving legal entity status and legal agreements between organisations in the Application ● outline business plan
M3	30 September 2019	To include: ● legal entity status and legal agreements between organisations in the Application signed and agreed ● Material progress towards agreement on structure and governance of Cyber Security Council
M4	31 December 2019	To include: ● Agreed governance approach and legal status resolved ● agreed approach to communications and marketing of 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
M5	31 March 2020	To include: ● draft approach to Qualifications Framework ● draft Code of Ethics
M6	30 June 2020	To include:

		● vision statement and roadmap for the profession as a whole
M7	30 September 2020	To include: ● mission statement on how to develop next generation of cyber security professionals and boost diversity in the profession
M8	31 December 2020	To include: ● Developed proposals for, and early implementation of, a common Royal Chartered Status for individuals to aspire to across the range of cyber security specialisms ● Clear proposals for how the Code of Ethics would be applied and enforced fairly, robustly and consistently across signatory organisations
M9	31 March 2021	To include: ● 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 ● position paper on transitioning government initiatives to the profession

TABLE 3		
Deliverable	**Date**	**Description**
D1	30 June 2019	Quarterly Progress Report + Milestone 2
D2	30 September 2019	Quarterly Progress Report + Milestone 3
D3	31 December 2019	Quarterly Progress Report + Milestone 4
D4	31 March 2020	Quarterly Progress Report + Milestone 5

D5	30 June 2020	Quarterly Progress Report + Milestone 6
D6	30 September 2020	Quarterly Progress Report + Milestone 7
D7	31 December 2020	Quarterly Progress Report + Milestone 8
D8	31 March 2021	Quarterly Progress Report + Milestone 9

9 - How to apply

Applicants should submit completed application forms (Annex B) by 16:00 on 28 February 2018. Applications must follow the application form format however each application can be supported by a maximum of 10 sides of A4 of supporting documentation.

An Application should be submitted as a single Word or pdf file with a typeface no smaller that 11 point. Applications must be written in English. Applicants should make it as easy as possible for Assessors to find the information they require. Completed applications should be emailed to csprofession@culture.gov.uk by 16:00 on 28 February 2019.

All clarification questions in respect of the application process should be emailed to csprofession@culture.gov.uk. The deadline for clarification questions is 8 February 2019. Where appropriate, the responses to (anonymised) clarification questions will be made available to all potential bidders and posted on gov.uk.

We intend to run one or more briefing sessions in mid-January 2019. These will be designed to give prospective bidders the opportunity to ask clarification questions about aspects of the application process. Briefing sessions will be held in London and, if there is sufficient demand, elsewhere in the UK. If you are interested in attending one of the briefing sessions, please email csprofession@culture.gov.uk to register your interest and we will contact you in early January with further detail on date and location. Since space will be limited, it is possible that we may have to limit the number of representatives from individual organisations.

Following the award of the Grant, Applicants may request a debriefing which will be provided in writing by the Authority.

10 - Timeframe

The Authority has established the following indicative timetable:

Activity	Dates	
	Start	End
Issue RFP	21 December 2018	28 February 2019 at 16:00
Invitation to submit clarification questions	21 December 2018	8 February 2019
Deadline for clarification questions	8 February 2019, 16:00	

Deadline to submit Application	28 February 2019, 16:00	
Assessment of Applications	28 February 2019	15 March 2019
Assessment Panel and interviews	w/c 11 March 2019	
Applicants informed of outcome of Assessment Process	End of March 2019	
Grant agreement negotiation between the Authority and Preferred Applicant	29 March 2019	26 April 2019
Grant Agreement signed by the Authority and Preferred Applicant	29 April 2019	
Project starts	30 April 2019	

Whilst the Authority will make every effort to keep to this timetable, the dates should be taken as being indicative. Any significant or material changes to the timetable will be communicated via the cyber security profession gov.uk page.