UK Cyber Security Council RFP FAQs

<u>Funding</u>

Is the available funding that is mentioned in the RFP (£1M-£2.5M) inclusive of VAT?

If the claimant is claiming for goods and services which incur VAT and is recoverable by them, then this cannot passed to DCMS as part of the eligible expenditure. If the VAT is not reclaimable by the claimant, then it can be part of the eligible expenditure outlined as part of the bid for between £1m - £2.5m.

How much evidence would you expect to see as a reasonable amount to support each financial model?

This is for the applicant to provide an appropriate amount of information to support any response as set out on the application form. Assessors may follow up with requests for more detail if it is required.

Can you clarify whether the grant will need to be paid in equal instalments?

As set out in the guidance for applicants, the default position is for DCMS to provide grant funding in eight installments over the two financial years. However, if an applicant can present a reasonable case for a differing drawn down structure, please include this in your application for consideration.

Are the funding scenarios set out on the 'Request for Proposals' the only scenarios bidders should consider?

Yes, these are the only scenarios which bidders should be consider when completing the application form.

Does Government have a particular preference on the three funding models which are presented in the RFP?

There is no further information or preference on funding scenarios available at this stage, outside of what has been highlighted in the guidance for applicants documents.

Is there a limit to the percentage of grant funding can be used to subcontract elements of the project?

We are not prescriptive as to how much of the funds could be subcontracted to additional suppliers outside of the primary supplier and potential consortium partners. If there are any elements of your application that are to be subcontracted, please clearly state the reasoning and financial arrangement that you propose. The applicant is responsible to ensure any third party is compliant with the standard Grant Terms and Conditions.

The approvals process reserves the right to challenge what elements of the work can, or should, be subcontracted..

Assessment

Will there be one single assessor for each application?

Each application will be read and scored independently by a minimum of three members of the Assessment Panel.

There are a number of options for which legal entity will underpin the council. Are you looking for a not for profit entity?

Applicants should set out in their application their proposed entity and outline why this is the best fit to meet the requirements.

There is a maximum of 10 sides of A4 supporting documentation. Are partner agreements part of that 10?

We would not consider agreements between different partners as part of the limit.

Where should applicants demonstrate their Cyber Essentials certification or provide evidence that they are obtaining this certification?

This should be stated in the supporting documentation.

Other questions

One of the key milestones is to obtain Chartered Status by December 2020. Would an application 'in process' suffice?

The applicant would need to set out a clear ambition and plan for the design phase of the new UK Cyber Security Council. It is expected that a request for proposals application would present an approach and understanding for how royal charter status can be obtained, or be in the final stages of being obtained, by December 2020.

The application can refer to 'in process' thinking where the applicant deems appropriate, but assessors reserve the right to request additional information and clarification as deemed necessary.

Is the requirement for the new UK Cyber Security Council to achieve Chartered Status to issue to individuals or is it to ensure that the Council itself has Chartered Status?

As set out in the government response, 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.

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.

How will Council ensure that the Code of Ethics it delivers can be kept up to date?

We leave this for the applicants to consider and present their approach in the application form.