working in partnership

Crown Commercial Service

National Cyber Security Centre
a part of GCHQ

Cyber Security Services 2

Buyers guidance (RM3764ii)

6100-19 (Sep 19)

Working with the National Cyber Security Centre (NCSC) to provide central government and the wider public sector with access to quality assured and certified cyber security services.

Contents

1

Key facts summary

If you are a public sector buyer, our Cyber Security Services 2 framework is the perfect solution for your security needs. Whether you are looking to quickly respond to a cyber-attack, or long-term threat prevention, we have it covered.

Here are some of the reasons why:

- All live suppliers on this agreement are certified by the NCSC, giving you confidence in the quality of service
- Access to a wide range of penetration testing, incident response, tailored evaluation and certified cyber security consultancy suppliers
- More and more suppliers will be added to the agreement as they complete their NCSC certification
- The agreement is compliant with the Public Contracts Regulations 2015
- It reduces your timescales – no further OJEU process needed
- Flexible call-off contracts (agreements between you and the supplier) can be up to 3 years to help with more complex requirements
- Suppliers have already submitted maximum day rates and duration based volume discounts
- High SME pariticipation and regional suppliers, supporting social value
- Short, medium and full tender mini competition templates depending on your timescales and requirements
- Simply fill out your requirements and let the suppliers tell you how they'll deliver it
- Terms and conditions have been specifically created based on an agile approach
- Government owned intellectual property rights means that you can continue to develop yourself or with any third party, or share and re-use

2

What is Cyber Security Services 2 Agreement?

As cyber attacks become more frequent and sophisticated, the public sector in particular needs to lead the way in ensuring that their systems are safe, secure and protected.

Building upon the first Cyber Security Services framework, the Cyber Security Services 2 framework is an EU compliant, and regulated central route to market for public sector customers to buy NCSC certified cyber security services. Using this agreement will ensure that your supplier will have been rigorously evaluated by NCSC, the national technical authority for cyber security in the UK.

Together with NCSC we have expanded the certified services on offer in this iteration of the framework, to better meet the current needs of public sector organisations.

3

What services can I buy?

Services available under Cyber Security Services 2 are split across 4 lots:

Lot 1: Certified Cyber Consultancy

- 1.1 Risk Assessment
- 1.2 Risk Management
- 1.3 Security Architecture
- 1.4 Audit and Review
- 1.5 Incident Management

Lot 2: Penetration Testing (CHECK)

Lot 3: Cyber Incident Response (CIR)

Lot 4: Tailored Evaluation (CTAS)

Lot 1 Certified Cyber Security Consultancy

Lot 1.1 Risk Assessment

This lot is for buyers who want to identify, analyse and evaluate the cyber security risks associated with the technology systems they are seeking to manage. Suppliers can help with each of these assessment stages to elicit and understand risk in support of management decisions.

Lot 1.2 Risk Management

This lot is for buyers who want to manage the cyber security risks associated with their technology systems. Suppliers can help you to determine pragmatic and effective means of managing your assessed risk (typically through treatment using a range of different control-types). This can help you gain confidence from these management activities.

Lot 1.3 Security Architecture

This lot is for buyers who want to ensure that the design and build of technology architecture is secure. Suppliers may design, or contribute to teams designing, systems and services to manage identified cyber security risks.

Lot 1.4 Audit and Review

This lot is for buyers who want independent assurance about the effectiveness of their cyber security arrangements. Suppliers can help by conducting checks, audits and reviews to confirm the current status. Suppliers can also identify potential weaknesses and recommend improvements to satisfy or maintain compliance, certification or broader policy requirements and remove any inefficiency.

Lot 1.5 Incident Management

This lot is for buyers who are looking to invest in policies and processes, which will help to improve resilience, support business continuity, improve buyer and stakeholder confidence and potentially reduce impact of a cyber incident.

Lot 2 Penetration Testing (CHECK)

This lot is for buyers who want to test for any vulnerability in their existing security systems. A CHECK service provider can analyse the systems or networks you rely on to carry out your business securely and effectively. They do this by conducting a number of tests designed to identify weaknesses, utilising publicly known vulnerabilities and common configuration faults. You will receive a report detailing any vulnerability and recommending effective security countermeasures.

Lot 3 Cyber Incident Response (CIR)

This lot is for buyers who are responding to a significant cyber incident. Suppliers are likely to be required to determine the extent of the incident and work towards managing immediate impacts. Additionally, they may provide recommendations to remediate the compromise and increase security across the network.

Lot 4 Tailored Evaluation (CTAS)

The NCSC Tailored Assurance Service (CTAS) provides assurance on the IT security aspects of a system, product or service. The tailored evaluations address specific assurance questions posed by accreditors on behalf of risk owners. This better enables risk owners to make informed risk management decisions. Buyers will have a clear requirement from government and a government sponsor, and could include Ministry of Defence (MOD), Critical National Infrastructure (CNI) or the public sector.

Check out these essentials before you apply for a tailored evaluation:

https://www.ncsc.gov.uk/articles/ctas-pre-application-checklist

Top Tips:

For further information on services, take a look at the NCSC marketplace

https://www.ncsc.gov.uk/

What is out of scope?

This framework excludes the following services:

- Any/all hardware and infrastructure
- Hosting
- Software/software licensing
- Networks or connectivity services

Full information can be found in the OJEU contract notice:

http://ted.europa.eu/udl?uri=TED:NOTICE:382951-2016:TEXT:EN:HTML&src=0

4

Our 4 Buying Options

There are four ways to run your mini competition under this agreement. Which option is best for you depends upon your project timescales and the complexity or scale of your needs.

Depending on which route you choose, you can ask suppliers to provide:

For more details on each option see Section 7 Running a mini competition, or the Cyber Security Services 2 webpage: https://www.crowncommercial.gov.uk/agreements/rm3764ii

Top Tips:

Crown Commercial Service can provide you with templates for each option and guidance throughout the mini competition process.

5

Buyer Scenarios

Scenario 1:
An NHS trust holds critical data on its systems. An attack on these systems could cause huge damage and delays to providing vital services. The trust wants to test whether its current system is secure.

Route:
Lot 2: Penetration Testing
Lot 2 suppliers can conduct a number of cyber security tests on the systems and networks you rely on. You will receive a report detailing any vulnerability and recommending effective security countermeasures.

Scenario 2:
A local police force is currently relying on a legacy system to protect sensitive information. It is looking to update the system to add new functionality and ensure that the information is adequately protected.

Route:
Lot 1.3: Security Architecture
Based on your requirements, suppliers can contribute to the secure design of system architectures. This can include guidance on adoption of common security architecture patterns, design principles and good practice, to the secure development and build of systems and services.

Scenario 3:
A county council is designing a new programme to help deliver public services. The service needs to share health and social care data to make them more productive, efficient and integrated. The security of the data is essential – it will be personal and sensitive in nature, so the county council must satisfy its regulatory obligations under the Data Protection Act.

Route:
Lot 1.1 Risk Assessment and Lot 1.2 Risk Management
Certified suppliers can work with your project team helping you to identify and tackle cyber security risks relevant to what you are doing and what you are trying to achieve.

6

Searching for suppliers

Before you run your mini competition, you can find out which suppliers could meet your requirements using our supplier search document.

The supplier search document shows:

- The lots each supplier is certified for (and therefore the services they can provide)
- The geographical locations suppliers can work in
- The industries or sectors suppliers have expertise in
- Supplier maximum day rates

Use this document to shortlist which suppliers you will invite to bid on your mini competition. **All eligible suppliers must be invited to bid.** You may not uses maximum day rates to de-select suppliers.

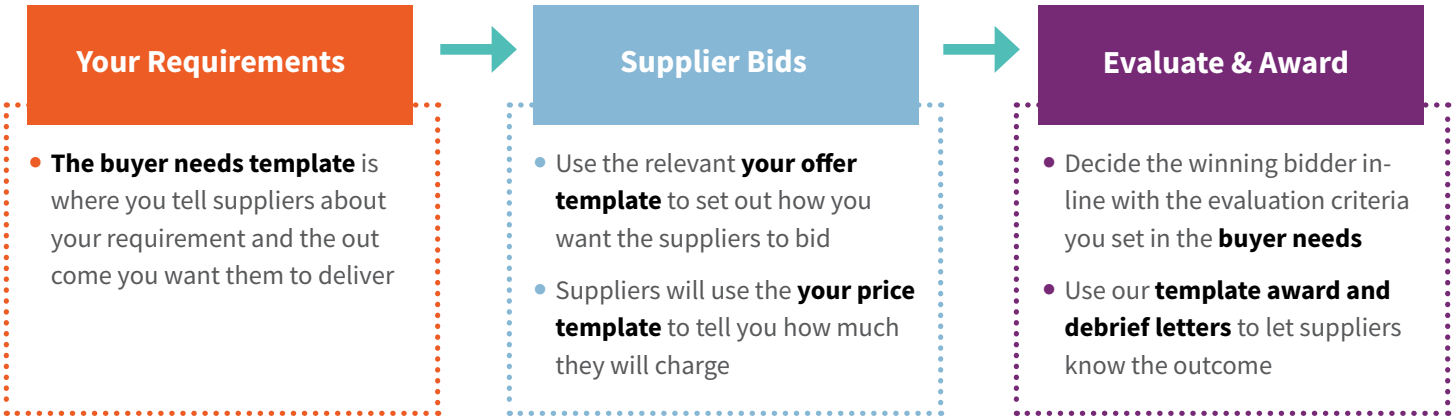
Top Tips:

When you have completed your mini competition, you can use the supplier search document to compliance check suppliers' bids

7

Running a mini competition

Buyers who want to use the Cyber Security Services 2 Agreement have to follow a mini competition process. Depending on which of 'Our 4 buying options' you decide to use, suppliers are required to tell you how they plan to deliver your requirement and how much they will charge to do so.



Mini competition overview:

This process is explained in the 5 simple steps below:

Step 1 Identify your needs

Identifying and defining your user and business needs is a crucial stage of the mini competition process.

At this stage, you will need to:

- Get any spend approval which may be required
- Complete the 'Buyer Needs' template outlining your requirement
- Decide on which of 'Our 4 buying options' you will use
- Complete the relevant 'Your Offer' template with what you want to ask the suppliers
- Explain how you will evaluate and score the supplier bids, clearing describing your evaluation model, criteria and their relative importance

Top tip: Document templates can all be downloaded from the agreement webpage
At this stage, you also need to set your project timescales. Make sure you allow suppliers time to prepare and submit their bids, especially on more complicated requirements. You should include precise details of the closing time and date in the 'Buyer Needs' so suppliers are clear on their deadlines.

Also within the 'Buyer Needs', you will need to tell the suppliers how you will be evaluating their bids – so clearly describe your evaluation model, including criteria and their relative importance.

Step 2 Launch your mini competition

Using the supplier search document, invite all eligible suppliers to bid against your requirements. During this mini competition process you must keep an audit trail of any dialogue and communication with the potential suppliers. This can either be done via your own procurement system or utilising the free CCS eSourcing tool.

CCS eSourcing tool can be accessed via this link:

https://crowncommercialservice.bravosolution.co.uk/web/login.html

The eSourcing tool contains a RM3764ii template, which contains all the documents/templates you will need for your mini competition, as well as all the suppliers 'live' on this agreement. These documents are also available on the agreement webpage.

Top tip:

All eligible suppliers must be invited to bid for your opportunity. The suppliers on this agreement are able to select which further competitions they participate in. If suppliers choose not to bid for your business, they should inform you of this as part of the procurement process.

Top tip:

More guidance on how to use the eSourcing tool can be found here:

https://www.gov.uk/government/publications/esourcing-suite-guidance-for-customers

Step 3 Clarifications

While your mini competition is live, we recommend setting a clarification window to provide potential suppliers with the opportunity to ask questions about your requirement.

All questions asked and their responses must be published to all potential suppliers.

Top tip:

CCS recommends, and can help you run and capture, a Q&A webinar session to address these clarifications.

Step 4: Evaluation

During your bid evaluation, you must treat all suppliers equally and fairly using the most economically advantageous tender (MEAT) criteria. It is also vital that you keep an audit trail and ensure that you have evaluated all bids in the same way you stipulated in the evaluation criteria.

Guidance on the evaluation criteria and weightings can be found in the relevant 'Your Offer' document.

Step 5: Award

Stages of the award process

Intent to Award

Issue 'Intent to Award' letter to successful supplier, and debrief letters to the unsuccessful bidders. These letters are not a formal commitment.

Standstill

Once you have identified the winning bid, we recommend you apply a standstill period - usually a minimum of 10 working days.

Award

After the standstill period, the Call-Off Contract can be sent out to the winning supplier and the contract is officially awarded.

You must tell all the suppliers of the outcome of the mini competition via email or letter, and should provide feedback to unsuccessful suppliers detailing the relative advantages of the successful bid. Providing feedback is part of the EU procurement regulations and it is also invaluable information for suppliers, which may help them improve their future bids.

Top tip:

CCS can provide templates for your evaluation reports, award and debrief letters.

You are now ready to award your contract. Engage with the successful supplier to develop your Call-Off Contract and to begin the project.

Publish to Contracts Finder

Once you have awarded the contract, you should visit https://www.gov.uk/contracts-finder and publish your award.

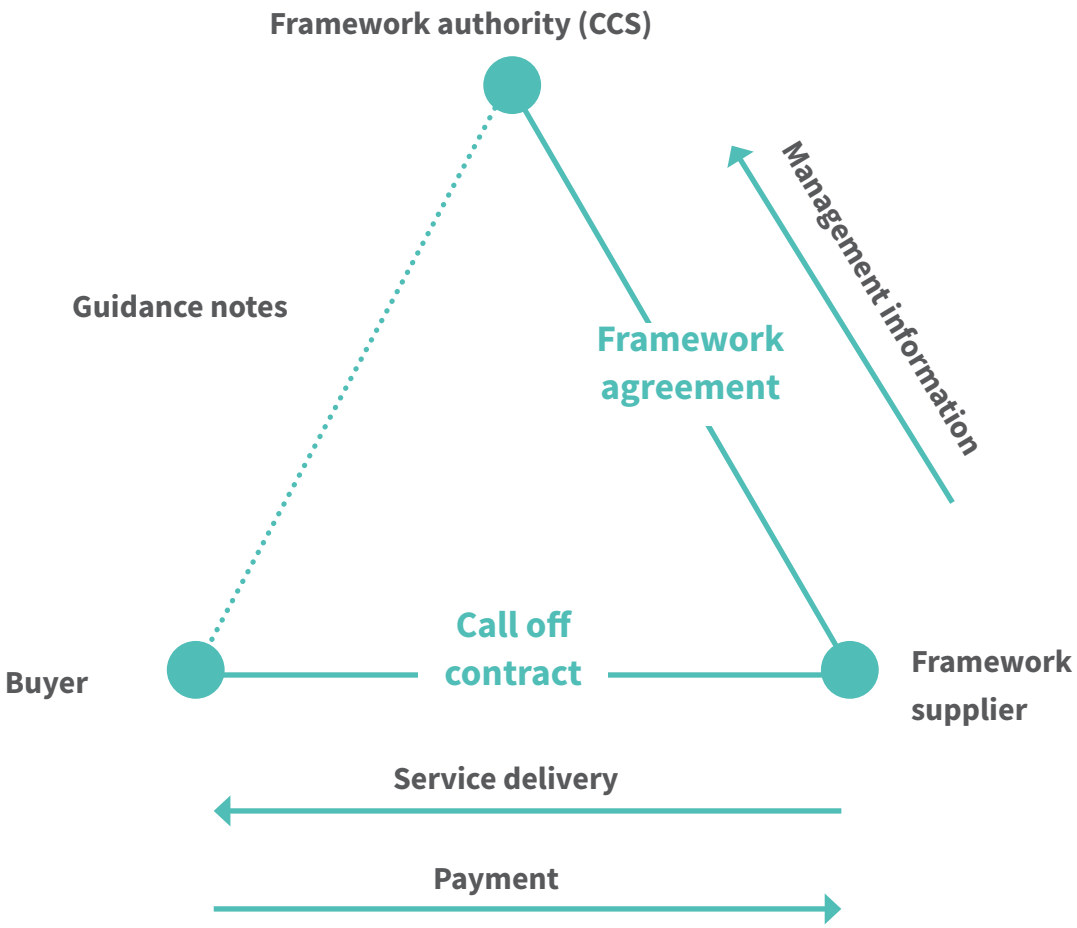
You must also advise CCS of successful award; see Section 10 Savings.

NB. Non-compliant buying will directly impact the legality and reputation of the framework and is strictly prohibited. Buyers who do not follow the correct buying processes will be at risk of legal challenge, fines and claims for loss of earnings, and the terms of the framework may be null and void in these cases.

8

The Call Off Contract

The Call Off Contract sits between the buyer and supplier and governs the purchase and delivery of the services. It is entered into by the buyer and the successful supplier, once the contract has been awarded.



How does the call-off contract' work?

Top Tip:

Building on feedback from Cyber Security Services 1, for this agreement we have increased the maximum call off contract length from 2 years up to 3 years. Buyers will specify the contract length within their 'Buyer Needs'. The option of longer contracts will give you more time with suppliers, to deliver more complex projects. For simpler, short service projects we recommend shorter contract terms.

The call-off contract is made up of three parts:

Part A (variable)
The order form (an overview of the services to be provided throughout the lifetime of the agreement) and the specific terms (which are specific to this contract)

Part B (variable)
Schedules (the buyer's requirements, the winning supplier's bid and the agreed work to be carried out)

Part C (non-variable)
Standard RM3764ii call-off terms and conditions

Parts A and B are the variable terms which are specific to you, the buyer, and your requirement. The standard terms in part C are specific to this agreement and are non-variable. When applicable, the buyer's specific terms will supersede the standard terms.

As part of tendering, each supplier has accepted the terms and conditions which make up the call-off contract. The suppliers cannot vary these terms, propose additional terms nor insert any of their standard terms of business.

The call-off contract templates can be found on the Cyber Security Services 2 webpage.

https://www.crowncommercial.gov.uk/agreements/rm3764ii

Any document or communication that is not as described in the templates will not constitute a call-off contract

Top Tip:
Providing the buyer has followed the correct buying procedure, the buyer has the right to not make an award. The buyer may also cancel the award procedure at any time. The buyer is not obliged to award any call-off contract.

9

Case Studies

For more complex requirements or where a buyer has a good news story, we encourage and urge customers to share their experience. One way to do this is via a case study. There is a simple case study template that can be found under the ‘documents’ tab within the Cyber Security Services 2 webpage.

https://www.crowncommercial.gov.uk/agreements/rm3764ii

10

Savings

Once you have completed your mini completion and awarded your call-off contract to the successful supplier, we want to hear from you! We have developed a benefits methodology to help CCS capture and measure savings.

This is a vital part of the mini competition process, and critical to CCS as a framework authority. It can help us to identify where savings are being made and where we could do more. Additionally, it can help you as a public sector buyer to demonstrate value for money.

Once you have completed your award, you must complete the customer benefits record, which can be found here:

https://goo.gl/forms/0sL5xfGvbr2EEaZQ2

(or find the link on the Cyber Security Services 2 webpage)

This brief form requires you to fill in very basic information about your organisation, the successful supplier and the contract awarded, to enable NAO Auditable savings reporting.

11

Templates and documentation

All templates and documentation can be located under the ‘documents tab’ within the Cyber Security Services 2 page via the following link:

https://www.crowncommercial.gov.uk/agreements/rm3764ii

12

Contact details

Crown Commercial Service (CCS)

cloud_digital@crowncommercial.gov.uk

0345 410 2222

National Cyber Security Centre (NCSC)

www.ncsc.gov.uk

You can also learn more about what we offer online:

www.gov.uk/ccs

@gov_procurement

Gov Digital Future

Crown Commercial Service