RM3764iii Cyber Security Services 3

Customer Guidance

Contents

1. Introduction

This guidance has been produced by Crown Commercial Service (CCS) to help you understand what Cyber Security Services 3 is and how to use it via the Dynamic Purchasing System (DPS).

This guidance document covers:

- How to use the marketplace to identify a supplier list
- What to include in your specification
- The information you need to provide when issuing a call for competition
- Managing your contract with your appointed supplier

The guidance provides you with the best practice approach to using the agreement. If you have a particularly complex requirement, you may wish to seek additional advice from your own commercial team.

1.1 What is the Cyber Security Services DPS?

This agreement replaces RM3762.ii Cyber Security Services 2. Following market engagement with both customers and suppliers, it was felt that a framework agreement was not flexible enough to reflect the rapidly changing Cyber marketplace. To address this, we are pursuing a new approach via this Dynamic Purchasing System (DPS) that will enable customers to access a range of suppliers offering a variety of Cyber Security services and provides suppliers with a route to market which is adaptable as their capabilities develop.

The principal benefits of using the agreement are:

- Agility and flexibility to meet the public sector's cyber security requirements
- Accessible route for suppliers to apply to join at any time
- A dynamic list of suppliers can be filtered, giving customers flexibility based on requirements
- The filter system enables the right suppliers to be matched and hear about the right opportunities
- Quality and price can be assessed based on an individual customer's requirement
- A dynamic pool of suppliers that can grow and evolve with the market
- Fully compliant with UK and EU regulations

1.2 Who can use this agreement?

This agreement can be used by all UK public sector bodies which includes:

- Central government departments, arm's length bodies and executive agencies
- Non departmental public bodies

- Devolved administrations
- NHS bodies
- Education, including universities, colleges, schools, academies, and further education providers
- Fire and rescue
- Local authorities
- Police
- Not for profit (charitable)
- Housing associations

1.3 The basic process

It is important to note that there is no option for direct award with a DPS. A buying organisation MUST run a further competition.

Appointing a supplier through the Cyber Security DPS includes the following key steps:

1. Define your objective and the requirements you are trying to address (including the level of assurance your organisation needs).

2. Develop your written specification

3. Use the DPS to obtain a supplier shortlist

4. Option of using a Capability Assessment to identify the suppliers that can meet your requirements

5. Issue your final specification, evaluation criteria and associated weightings to identified suppliers

6. Receive and evaluate written proposals from suppliers

7. Inform unsuccessful suppliers providing feedback and evaluation scores

8. Option to conduct a face-to-face presentation and evaluate

9. Award the contract to the successful supplier and confirm the award to CCS

10. Provide feedback and evaluation scores

1.4 The role of CCS

Our role is to provide you with advice and guidance to help you get the best outcome from the marketplace. We can help with any queries you may have, such as the best way to

appoint a supplier and advice on structuring your evaluation criteria and how to structure your contract.

CCS manages the overarching marketplace and the suppliers at agreement level. You are responsible for managing the contract with your appointed supplier. However, CCS is able to help with any issues you may have that require escalating, see **Section 5 Managing your contract** for further details.

If you have any other queries please email us at info@crowncommercial.gov.uk or call our Customer Service Desk on 0345 410 2222.

2. What can I buy?

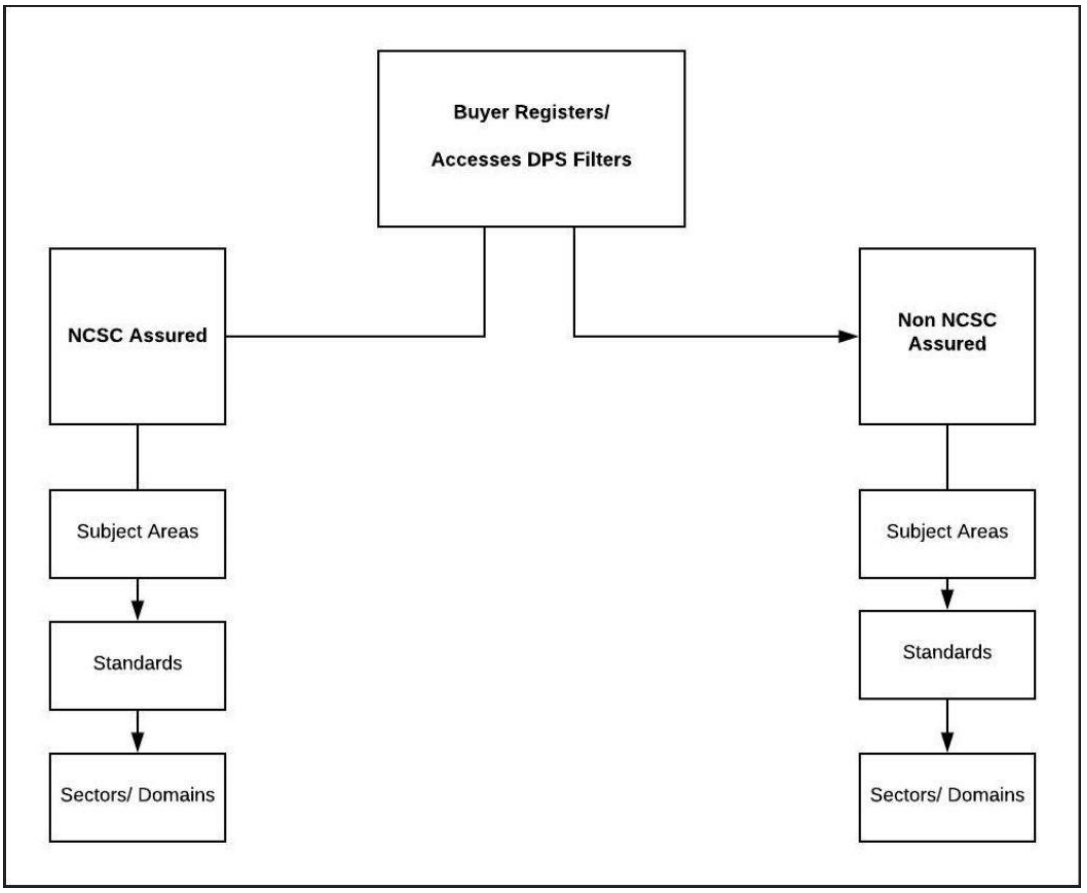
The Cyber Services 3 DPS Agreement provides public sector buyers with the opportunity to procure an extensive variety of Cyber Security services from a range of suppliers. Details of how to use the DPS itself are found in section 4.

2.1 NCSC vs Non-NCSC Assured

This DPS offers two distinct routes to finding a pre-qualified set of suppliers who offer a range of cyber security services. The first route provides the buyer with suppliers who are assured by the National Cyber Security Centre (NCSC). Using this filter will ensure that your supplier will have been assessed by NCSC, the National Technical Authority for cyber security in the UK (see section 3 for more information).

The second route provides the buyer with a set of suppliers who provide similar services to those under the NCSC assured route but without the assurance the National Technical Authority provides. It is therefore the responsibility of the purchasing authority to determine whether the service offered is fit for purpose. This may involve understanding what is assured by other accreditation bodies and how they are tested.

This is the first filter that you as the buyer will be presented with. Both journeys mirror each other, however, on both sides there will be some filters that are greyed out depending on whether or not they are applicable. The below diagram highlights the two distinctive journeys.



CCS will ask for proof of NCSC certification when a supplier joins the DPS. You do not need to worry about asking for evidence at the call-off stage.

2.2. Subject Areas

The category/service type column in the table below is the next filter set you will encounter when using the DPS (referred to as subject area in the DPS). We have included a description of the services below but please note this description will not be present on the DPS.

Depending on what you select in the first filter (NCSC or non-NCSC assured) you may encounter some filters which are greyed out in the DPS, this is because they are not provided for under the option you have chosen.

Category/ Service type		Service Description/ Example
Consultancy and Advice	Risk Management	Documenting risks to help Buyers identify and tackle relevant security risks.
	Risk Assessment	Recommending how to manage cyber security risks.
	Audit and Review (including evaluation and testing).	Identifying, testing and evaluating risks. Reporting outcomes to show compliance with internal and external policies and procedures.
	Security Architecture	Designing and developing security architectures that take account of business outcomes
	Certification. e.g. Cyber Essentials	Assessing compliance with regulatory and industry compliance standards
	BCDR	Providing advice and strategies to help organisations build resilience and respond to disasters, including research, impact assessment, testing and training.
	Training	Providing training covering different aspects of cyber security.
	Policy Development	Providing advice and review of IT security policies.
Penetration test / Health check	Penetration Testing/Pen test	Testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.
	Check	Penetration testing offered by NCSC approved suppliers who use an approved methodology and provide reports to a specific standard.
	IT Health Check	Checking of IT systems to identify vulnerabilities and recommend remedial action.
Incident Management	Incident Response	Fast action response to cyberattacks, providing recommendations to deal with the compromise and mitigate risks.
	Disaster Recovery	Providing advice and producing disaster recovery plans.
	Threat Intelligence	Providing advice on cyber threats drawing upon intelligence from appropriate sources.
	BCDR	Providing range of advice and support covering business continuity and disaster recovery planning and responses.
Data Destruction	Secure data removal and IT sanitisation services.	Secure data erasure and disposal of IT media and assets using audited destruction procedures.

2.3. Additional Filters

Buyers may also apply the following Filters as part of their Order Procedure. Suppliers must be able to demonstrate the relevant accreditation, standards, compliance or experience to satisfy the requirements of the relevant Filter.

Accreditations and Standards

Cyber Essentials Plus
Crest/ Cyber / Tiger/ Other
PCI Assessor
Project Management – APM Qualified
Project Management – PRINCE Qualified
Clearance: Counter Terrorist Check
Clearance: Security Check
Clearance: Developed Vetting
NPPV (1,2,3)

Experience

Experiences:
Networks
Database
Internet
Cloud
Premises
Endpoint / applications
GDPR
Other

Sectors

CNI Emergency Services:
Police
Ambulance
Fire Services
Coast guard
Other

Critical National Infrastructure: (CNI)
Chemicals
Civil Nuclear Communications
Defence
Energy
Finance
Food
Government
Health
Space
Transport
Water
Other

2.3. What is out of scope?

This agreement excludes the following services:

- Any/all hardware and infrastructure NOT specifically required to deliver the Cyber Security Services in the Filter Categories covered by this Contract.
- Hosting
- Software/software licensing NOT specifically required to deliver the Cyber Security Services in the Filter Categories covered by this Contract.
- Networks or connectivity services

2.4. Cyber Security Services DPS and other CCS agreements

- **G-Cloud** All NCSC certified services and suppliers are out of scope of G-Cloud (including through subcontractors). G-cloud is on supplier terms, Cyber Services 3 will in most cases provide more competitive pricing due to the need for a further competition.
- **Digital Outcomes and Specialists and TePAS** The only cyber security services that would go through this agreement would be those offered as part of a wider service offering (not a standalone service).

3. National Cyber Security Centre (NCSC) assured services

The NCSC is the UK's National technical authority for cyber security incidents. It was formed in 2016 to provide a unified national response to cyber threats. The UK's National Cyber Security Strategy 2016-2021 outlines the Government's intent behind setting up the NCSC.

The NCSC offers assurance that covers a range of services. Customers purchasing services offered by NCSC certified suppliers can be assured that they meet the National Technical Authority's technical standard. CCS are working closely with NCSC to ensure that customers are fully aware of the NCSC certifications and what this means for you as a buyer.

What are the benefits of using an NCSC assured service or supplier?

- It has met the NCSC's standards and can be trusted to act in NCSC's name.
- It has a proven track record in delivering high quality consultancy services to customers;
- It has demonstrated that it has a defined process for working with customers to understand their needs and tailors advice accordingly;
- It has demonstrated a clear understanding of current and potential cyber threats and techniques and potential effective mitigations;
- It has demonstrated that it acts with integrity objectivity and proportionality; it protects the client's confidentiality and integrity and complies with relevant laws and regulations;
- It seeks to continuously improve the services offered to meet the evolving needs of the customer.

NCSC Certified Cyber Security Consultancy Scheme

Aimed at providing government, wider public sector and Critical National Infrastructure (CNI) with support on a wide and complex range of cyber security issues, the certified consultancies give customers independent, expert advice.

NCSC certification is designed to suit consultancies of all sizes and addresses the following functions:

- Risk Management
- Risk Assessment
- Security Architecture
- Audit & Review

Penetration testing (CHECK)

Penetration testing is designed to identify any weaknesses and common configuration faults in the systems and networks that businesses rely on. The testing company then recommends steps to counter any problems that are found. CHECK is the term for NCSC approved suppliers who offer penetration tests using an approved methodology and provide reports to a specific standard.

Penetration testing CHECK was developed for government departments, public sector bodies and the organisations forming the UK's critical national infrastructure (CNI). All these bodies should be using a penetration testing CHECK service provider to conduct any penetration tests on their IT systems. Penetration tests conducted by a CHECK provider that are not conducted formally as part of the CHECK scheme will not meet the CHECK criteria.

Cyber Incident Response (CIR)

Cyber Incident Response companies help organisations with networks of national significance who have been the victim of a cyber attack. The Cyber Incident Response scheme certifies companies which specifically deal with sophisticated, targeted attacks against networks of national significance. We advise that any Government organisation who has been a victim of a significant cyber-attack should be using a Cyber Incident Response certified company to ensure a comprehensive response to the incident.

Certified training

Designed to assure high quality training courses delivered by experienced training providers, courses are assessed at two levels:

- Awareness – introduction for those new to cyber security to give a thorough foundation on the subject
- Application - these courses are designed for specialists, professionals or practitioners within the cyber security field and provide detailed insights and understanding. They are most suitable for individuals already working within a cyber security role who wish to further their professional capability.

Topics currently offered on certified training courses include (please note these may change throughout the life of the agreement and will be updated accordingly):

- Certified Ethical Hacker
- Certified Ethical Hacker Cloud and cyber security
- CISSP
- Cyber Security Awareness
- Cyber Essentials and Cyber Essentials Plus
- Cyber First training courses
- Cyber security training for Boards, NEDs, Trustees and Auditors
- Cyber security training for CISOs and Senior Information Risk Owners
- EC Council Certified Security Analyst
- EC Council Certified Chief Information Security Officer
- Ethical hacking and digital forensics

- GDPR Awareness - Online
- Incident response and management
- Industrial control systems
- Information security management
- Maritime cyber security
- NIS Directive
- Threat assessment methodologies

For more information on any of the above please visit the NCSC website: https://www.ncsc.gov.uk/section/products-services/ncsc-certification or https://www.ncsc.gov.uk/information/certified-training

4. How Do I Buy?

4.1 Registering to use the Dynamic Purchasing System (DPS)

1 Follow this link: https://supplierregistration.cabinetoffice.gov.uk/organisation/register

(note although the link says Supplier Registration, this is where both Suppliers and Buyers accounts are held).

2 Select Buyer

3 Select Next

4 Complete your details, including organisation name and email address.

5 Confirm acceptance of the terms and conditions and submit.

6 The registration request will then need to be accepted by the organisation's User Manager in order for the user to be granted buyer access. If there are no active User Managers registered to the relevant organisation, the user will be granted access without this confirmation. In the eventuality that the organisation does not exist within the Supplier Registration Service, the request will be forwarded to CCS for approval before being registered as a public sector organisation on the platform.

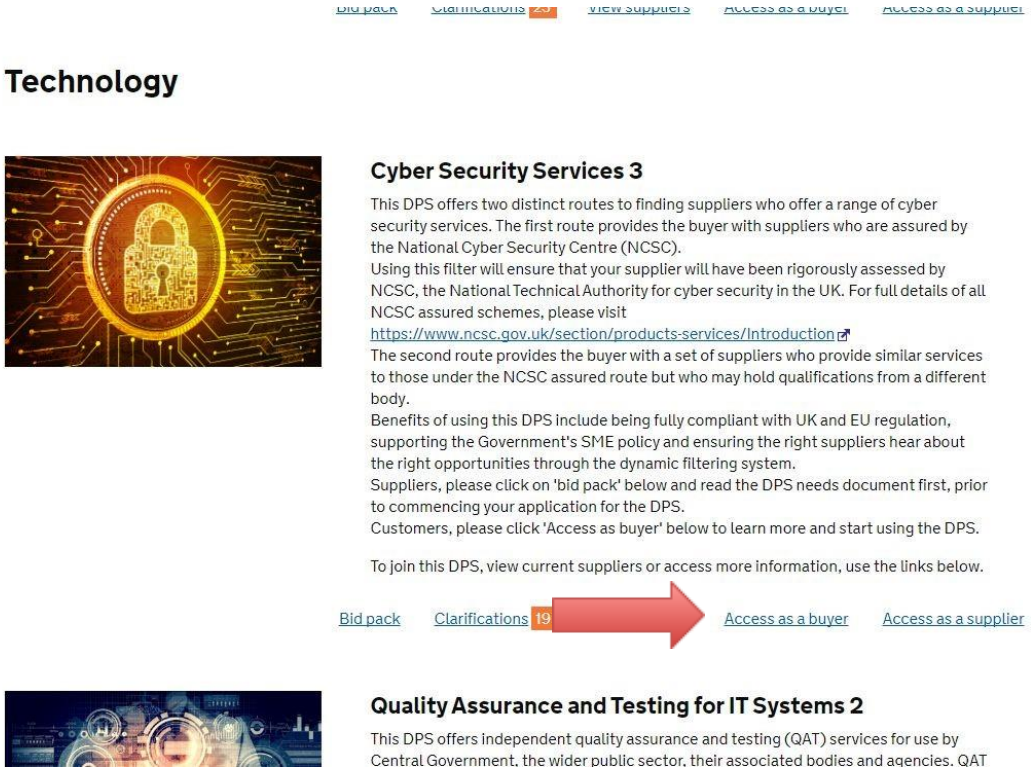
7 You will receive an activation email once you have completed the above registration process (and the registration request has been accepted), containing an activation link needed in order to set a secret security question and answer, and a password to login.

4.2 Obtaining a supplier shortlist from the DPS

1 Go to the DPS homepage: https://supplierregistration.cabinetoffice.gov.uk/dps

2 Navigate to the Cyber Security Services 3 marketplace by clicking on the Technology header (see below screenshot).

3 Choose the 'Access as a buyer' option and confirm your acceptance of the customer access agreement



4. Log in to the system
5. Click on 'create new category export' in the bottom right hand corner and use the filters to reflect your specification and create your supplier shortlist
6. Save your filtered shortlist by clicking on 'Save category' and give the shortlist a unique name specific to your competition. Export the list of suppliers from the marketplace.

Important: We recommend that the exported supplier list is used within 2 working days, as new suppliers may be added at any point, thus changing the list of suppliers eligible to compete. Please refresh your final list as necessary.

4.3 Capability Assessment (Optional)

You can start your call for competition using a capability assessment stage, this will help you to identify which suppliers from your shortlist are going to be the most suitable. As part of this process, you might decide to hold an engagement day with suppliers in order to discuss your requirements in more detail.

You may wish to run this process to refine your shortlist or to assess if any suppliers are capable of meeting your requirements.

You can use a series of 'yes' and 'no' questions that are mandatory for suppliers to pass to get to the written stage - you could, for example, use the ability to meet your stated deadline as a question.

Please use questions that relate to key requirements only at this stage, and not those that you would like to score in the main tender stage.

You do not need to send the final specification to suppliers who have deselected themselves, or not engaged in the capability assessment, unless you make material changes to the specification as a result of the exercise.

We have included a template capability assessment on our webpage which you can amend to meet your needs (or you can use your own).

4.4 Things to consider when drafting your specification

The below are things that you might want to consider specifically for a requirement under this DPS. Annex 2 provides more general specification writing guidance.

Evaluation and weightings

DPS Order Schedule 7 – Order Procedure which is available in the documents section on the Cyber 3 webpage details what you as a buyer and what the supplier need to do to ensure the correct process is followed when running a further competition and placing an order under the DPS. At the end of the Schedule there are details of the weightings you can use, within the ranges stated it is up to you as the buyer how you allocate the weightings.

Pricing structure

You will need to state what charging structure you want the supplier to adhere to within your specification. Within the agreement, CCS has suggested that this broadly aligns with the SFIA framework, however, you as the buyer need to be clear on what you are expecting from the supplier and how you are expecting to pay for this i.e. will it be output based, on completion of contract, after a certain milestone etc.

Standards

As a minimum, all suppliers on this agreement will be Cyber Essentials certified. However, do you have any specific standards which you require from your supplier? E.g. Do they need to have Cyber Essentials Plus? Do you require them to have project management qualifications? All of this will need to be clearly detailed in your specification.

Buyers need to consider the standards provided for within this agreement and what your organisation requires. You may want to do some prior research on the standards that are covered within this agreement to ensure you have an understanding of the cost benefit implications. If you would like further information please contact technology.solutions@crowncommercial.gov.uk.

Security and data management

You will need to detail your organisation's security requirements with regards to data handling in the specification. What do you require the supplier to have in place to protect data handled, processed or stored, are there any policy requirements (e.g. GDPR) as part of delivering the services? Do you need to specify where your data is to be stored?

Security clearance

Under this DPS agreement all suppliers are contractually required to have the Baseline Personnel Security Standard as a minimum. However, depending on the systems and data that the supplier and their staff may come into contact with, you may need them to have more stringent security checks and this will need to be stated in your specification.

Policy on T&S

You will need to be clear in your specification as to whether you want your suppliers to follow your organisation's travel and subsistence policy, if these are to be included in day rates and how you want staff and subcontractors to claim expenses.

Important: Please ensure you allow enough room for suppliers to respond adequately to your requirements (consider whether you are going to give suppliers a page/word/character limit for their response). Suppliers want to be open and transparent in their response and will want to list any assumptions associated with their bid and restricting responses can sometimes mean suppliers are unable to detail everything they need.

4.5 Issuing your specification

Your completed specification along with all other relevant documents, must be issued to all shortlisted suppliers, unless they have been deselected through a capability assessment. For advice and guidance on what to include in your specification please see Annex 2.

Please invite the contact listed in your exported shortlist to reach the right supplier contact.

This can be done either via the CCS online procurement tool (eSourcing), your organisation's own procurement tool or by emailing suppliers.

Using a portal gives an auditable approach to the tender process and is used to:

- Respond to clarification questions
- Track bid responses
- Send reminders to bidders
- Communicate to successful and unsuccessful suppliers

If you would like to use the CCS eSourcing Suite and have not previously used this to run a further competition, please contact eenablement@crowncommercial.gov.uk who will be able to set you up on the system and provide you with guidance on how to use it.

4.6 Reviewing proposals from suppliers

All suppliers will need to provide a written proposal in response to your specification.

Responses should not be discussed outside of the evaluation team and pricing information should be treated as commercially sensitive.

Make sure that you maintain a fully documented audit trail of the results and final award decision, which will be useful when providing feedback to the participating suppliers.

4.7 Face-to-Face presentation stage (optional)

After reviewing written proposals, you may choose to invite suppliers with the best written response to present their proposal as an opportunity for face-to-face dialogue.

A face-to-face presentation will allow suppliers to present more detailed proposals and answer any specific questions you may have regarding their written response.

It is also a great opportunity for you to meet the operational team and better understand the skills and expertise they will bring to your project.

If you decide to include a face-to-face presentation, you should outline from the outset of your call for competition how many suppliers you expect to invite, ideally three, and the criteria you are looking for and scoring them on.

You should only invite suppliers who have a realistic chance of winning the competition to the presentation stage.

The evaluation panel should prepare the structure of the meeting and it is recommended to share this with the shortlisted suppliers so that they are able to properly prepare.

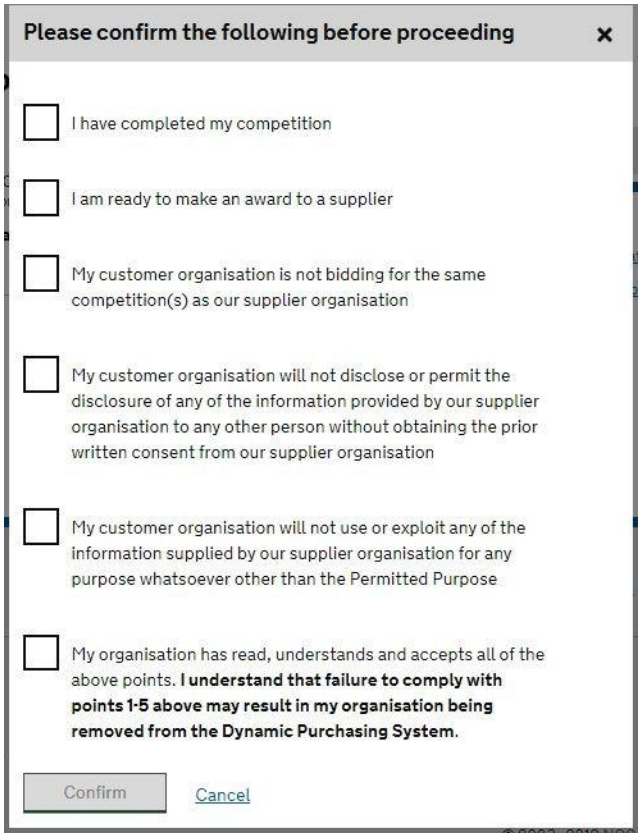
You will need to keep documentary evidence of how you have scored the presentations and will need to ensure you are as far as possible giving each supplier the same information.

4.8 Awarding the contract

As part of your compliance check before awarding your contract, you have the option to request evidence of contract examples, insurance and cyber certificates provided by the suppliers on the marketplace.

To do this, you will need to log-in to the marketplace and navigate back to your saved search. Find the supplier(s) you wish to see further information for and click on ‘see evidence’.

You will need to complete the following form on the DPS system to gain access to the evidence.



The suppliers will then be sent a notification and will give you access to see the evidence. Following the successful completion of your competition evaluation you can now award a contract to the successful supplier.

Once you have the relevant internal approvals in place, you can notify all participating suppliers of the outcome.

A standstill period is not mandatory but can be used voluntarily for high value contracts.

You **must** use the Order Form to create your contract, which is aligned to the contract terms set out in the agreement.

You can contact CCS for Word versions of the Order Schedules.

There are some sections of this contract that you can alter depending on your organisation and requirements.

The Order Form must be completed by the customer prior to being sent to the supplier for signature. The document includes guidance so you understand how to fill in the relevant sections.

Once your contract has been signed, you are required to send your award details to technology.solutions@crowncommercial.gov.uk including:

- Contract name

- Contract length (including any extension options)
- Contract total value
- Winning supplier name

Please remember to fulfil your organisation's transparency requirements and publish details of your award on Contracts Finder where necessary. (Customers need to sign-in via the link in the top right corner in order to post details).

The Procurement Policy Note relating to the use of Contracts Finder can be found here.

4.10 Providing feedback to suppliers

You should provide constructive, written feedback to all participating suppliers and include a full breakdown of their scoring.

Feedback comments should be objective and link back to the evaluation criteria. This will help suppliers understand how they can improve for future opportunities.

5. The Public Sector contract and the order schedules

The Cyber Security Services 3 DPS uses the CCS Dynamic Purchasing standard contract (part of the Public Sector Contract).

The maximum term for a call-off contract (order contract) under this agreement is 3 years including any extensions.

5.1 Core Terms

"Core Terms & Conditions" are the set of T&Cs applicable to both the DPS Contract and the Call-Off Contract. These terms have to be accepted by all potential suppliers when registering for the DPS and are non-negotiable.

5.2 Joint Schedules

"Joint Schedules" are the Schedules that apply to both the DPS Contract and Call-Off Contract / Order.

5.3 Order Schedules

“DPS Order Schedules” are those terms which apply to the call-off contract. Buyers are able to amend certain schedules (e.g. specification, pricing) based on their requirements. Please ensure your organisation takes time to consider these terms (e.g. pricing mechanism, service levels and security) as you need to be very clear from the outset what your terms and conditions are going to be. In order to enter into contract with a supplier you need to complete the Order Form. The template form can be found in DPS Schedule 6.

Below is a list of some of the key Order schedules and what is required.

Order Schedule 1 Transparency Reports – Central government bodies are subject to procurement transparency policy requirements. Where these apply to your organisation you should set out your transparency reporting requirements in the annex to the schedule, guided by Procurement Policy Note 1/17.

Order Schedule 2 Staff Transfer – Staff transfer provisions may be required for deals with a dedicated service provision element. You should review the schedule options against the circumstances of your procurement, taking legal advice where necessary. If Transfer of Undertakings (Protection of Employment) Regulations (TUPE) rules mean that a staff transfer is likely following award of your order contract you’ll need option A where buyer staff will transfer to the incoming supplier, or option B where the staff of an existing supplier will transfer to the incoming supplier. You’ll also need to consider whether part D (pensions) should be incorporated into the contract and if so which annex should apply – D1 (CSPS), D2 (NHSPS) or D3 (LGPS). Part C will apply if there will be no staff transfer at the start of the order contract. Where there’s the potential for a staff transfer at the end of the contract part E should be included to ensure that obligations are placed on the supplier to assist with the process.

Order Schedule 4 Order Tender – Include this schedule if you want to carry the commitments made in the winning supplier’s tender across into the order contract.

Order Schedule 5 Pricing – Include this if the Order Form doesn’t provide sufficient scope to readily capture the detail of your contract pricing.

Order Schedule 6 ICT Services – Some Cyber 3 contracts will need this schedule, if only for the inclusion of software licensing provisions associated with the services being provided. Other elements of the schedule, such as augmented due diligence and warranty provisions will mainly be relevant to contracts involving ongoing service provision With reference to paragraph 6, you’ll need to decide if you want your supplier to produce quality plans for your approval, the purpose being to ensure the deliverables are provided in a systematically-controlled manner in accordance with documented processes. Annexes A and B should be used to document any supplier software licensing terms. Such supplier terms sit at the bottom of the contractual order of precedence such that if there’s a conflict with any other element of the contract then it’s the latter that will take precedence.

Order Schedule 7 Key Supplier Staff – Decide if there will be certain supplier roles and personnel that will be key to delivery of your contract. If so, include this schedule in the contract and list the key roles with details of the Supplier staff to occupy those roles to be input before award. Specify the period of notice your supplier must give to move a key person from their post.

Order Schedule 8 Business Continuity & Disaster Recovery – Where your contract has a significant ongoing service provision element you should think about whether you need the assurance of a supplier business continuity and disaster recovery plan to ensure that disruptive events don't have a serious impact on the business operations to which the contract relates. If so, then include this schedule in your contract.

Order Schedule 9 Security – Firstly you will need to decide if you should include this schedule in your contract. Will there be any potential ICT security exposure associated with the supplier's performance of the contract? If so then one of the options in the schedule should be adopted. The Short Form version obliges the supplier to comply with: 1. the buyer's security policy 2. a security management plan which they must produce for buyer approval and which must set out how all aspects of the deliverables will be protected. It will be subject to annual review and updating. The Long Form option also obliges the supplier to implement an information security management system (ISMS) compliant with relevant standards and key government guidelines. This is to be tested and updated annually. You should note that unless you specify that you require a tailored ISMS then the supplier's ISMS may be an existing one covering their whole estate.

Order Schedule 10 Exit Management – Decide if the nature of the contract is such that there will be a need for a rigorous, systematic approach to contract end and transfer of responsibility for provision of deliverables to the buyer or a replacement supplier. If so, include this schedule in your contract.

Order Schedule 13 Implementation Plan & Testing – Schedule 13 ensures there is a clear contractual agreement on the roadmap for contract implementation where the complexities of this cannot be captured in the Order Form. The supplier will have produced an initial draft prior to award of the order contract. This initial draft will be updated for agreement by the buyer and incorporation into the contract thereby committing the parties to perform their obligations in accordance therewith The plan should include a suitable number of milestones – key contract implementation checkpoints at which the buyer must sign off satisfactory delivery of the requirements in respect of that milestone. You must approve the plan before it's implemented.

Order Schedule 14 Service Levels – If you use this schedule you'll need to decide; i. The service level performance criteria – what measures do you require? ii. The required minimum service level for each of these iii. Whether you want to apply a service credit regime under which the relevant charges will be reduced if the service levels fall below that required.

Order Schedule 18 Background Checks – You may want to use this schedule if your contract might involve supplier staff coming into contact with children or vulnerable adults, or if there are other sensitivities around past criminal behaviour. The schedule allows the buyer to specify that the supplier ensures that staff involved in performance of the contract are subject to, and satisfy, checks in respect of relevant convictions.

Order Schedule 20 Specification – You may want to use this schedule if you've carried out a competition and want to incorporate your specification into the contract (recommended).

Order Schedule 22 Secret Matters – This schedule contains government-standard provisions applicable to circumstances in which the supplier may be exposed to highly sensitive information.

Important: In due course we will be adding Word versions of the order schedules to our webpage. However if you need Word versions in the meantime, please contact Rachel.zabari@crowncommercial.gov.uk who will be able to send them to you.

6. Managing your contract

6.1 Your obligations as customers

There are a number of obligations we have as customers. These include:

- Providing a clear specification setting out your requirements (services and deliverables) and timelines for each phase of work
- Communicating with your supplier on a regular basis to discuss progress
- Promptly addressing any issues with your supplier
- Agreeing at the start of the project how frequently you expect to receive reports from your supplier, this should be in line with the requirements in your specification
- Pay your supplier within 30 days of approving the invoice. Check invoices against the rates and deliverables agreed in your contract

You should be able to rely on your supplier to give you expert advice and consultation that comes from its collective wisdom and experience.

A good supplier will explain its strategy, offer honest advice and acknowledge when the topic has shifted outside of its expertise. As a customer, you should also proactively advise the supplier on anything it needs to know to deliver the best results.

6.2 How to manage issues

By ensuring you have regular communication with your supplier you should be able to avoid any major issues. In the event that you do experience performance issues with your supplier, you should take the following steps to address the issue as quickly as possible.

1. Raise the issue with the supplier soon as possible
2. Clearly set out your concerns and agree a plan of action with the supplier including a deadline for resolution - put in place more frequent status updates if necessary
3. If the issue is not resolved by the agreed deadline, escalate the matter internally and to supplier directors
4. If the issue is not resolved by the agreed deadline, contact the CCS marketplace manager to notify them and agree next steps

5. If you have carried out all reasonable steps to rectify the issue, allowed time for recourse and are still not satisfied, then you will need to decide how to resolve the issue with internal colleagues and CCS

7. How to contact us

Email: info@crowncommercial.gov.uk
Telephone: 0345 410 2222

Annex 1

Timetable for appointing a supplier

The timetable below provides an example of the timescales that are involved in a call for competition, from the date of issuing your tender to contract award. Please engage with your commercial function when planning the timetable.

You should allow up to 6 - 8 weeks if you choose all recommended options. You may require more time for more complex, high value projects.

For situations where you are dealing with an incident, a shorter time-scale would be more appropriate, providing there is enough time to run the further competition.

Task	Required/ Optional	Task owner	Day	Week
Tender Issued	Required	Customer	1	1
Deadline for submission of Capability Assessment	Optional	Supplier	5	1
Evaluation of Capability Assessment	Optional	Customer	7	2
Shortlisted agencies from Capability Assessment notified	Optional	Customer	8	2
Deadline for the submission of clarification questions	Required	Supplier	11	2
Deadline for response to clarification questions	Required	Customer	13-14	2
Deadline for submission of proposals	Required	Supplier	18-19	3
Evaluation of proposals	Required	Customer	20-27	4
Award contract	Required	Customer	27+	5

Annex 2

Specification writing guidance

Drafting an outcome based specification

The section will take you through the following areas of developing your supplier specification.

A good specification should include all of the following:

1. Title

This notifies the reader of the focus of the project.

2. Summary

Use this section to set out the nature of the issue and the project specification to the supplier. The supplier should be able to use the summary to decide whether it would be appropriate for them to bid for your work.

Make sure you cover:

- A clear and specific description of the problem, explaining why the project is needed
- A short summary of your objectives
- Any mandatory service standards or policy requirement e.g. NCSC certification, Cyber
- Essentials Plus or particular project outputs
- Expected project length

3. Background to the issue

Use this section to provide detailed information on the background to the project.

Make sure you cover:

- Outline the issue the project relates to
- Explain who you are as a customer - don't assume the supplier knows your department/ organisation
- Set out any campaign or policy information the supplier needs to understand

4. Project objectives

What is the aim of the project?

This should be clear-cut, detailing the overall objectives plus a bullet point list of specific objectives.

If you already have SMART objectives you should include these here.

5. Outputs

The deliverables required, expanding on the high level outputs – such as any data, reports, any service levels and KPIs and the Intellectual Property position. Detail frequency of any reporting.

6. Timings

Give dates for awarding the contract, completion of the project – and any interim deadlines.

7. Form of proposal

A clear statement of how the proposal should be presented. This might include a list of headings for the proposal, the order of the headings and the detail required. e.g. *a proposal of a maximum of eight pages is required by [date].*

Consider whether you require CV's, proof of qualifications/ certifications etc.

The proposal should contain the following:

- A succinct summary of the proposal
- A demonstrable understanding of required outcomes [and sector]
- Your organization's experience of similar projects and [relevant] capability
- Details of the personnel to be involved including their role for this project and their relevant experience
- Arrangements for managing this work and quality assuring outputs, including how you would like to work with the customer during the project
- A detailed budget / costing, including a breakdown of time and costs per activity and per team member

8. Evaluation criteria

The basis on which the contract will be awarded including the weightings of the sections / questions. The criteria could include;

- Suitability of methodology
- Experience in the area
- Evidence of understanding the brief
- Whole life costs

Annex 3

Document checklist before issuing your call for competition

☐ State RM3764.iii Cyber Security Services 3 at the start of your competition document

☐ Tender timetable which sets out the high level stages of the process and when you intend to award and start the contract

☐ Tender timetable including dates for the clarification period, when suppliers have to ask questions by and when you will provide responses by.

☐ Detail on the process and evaluation of the Capability Assessment stage (if used)

☐ Detail on the process, evaluation and weighting of written proposals

☐ Appendices (if used)

☐ Draft letter of appointment and contract terms

☐ Tendering instructions (details on the submission process specific to your organisation)

☐ Procurement tool registration details (if inviting suppliers to your organisation's own portal)