# **Schedule 1.**

# **Specification**

## **1.1 Our priorities**

Crown Commercial Service (CCS) has key priorities:

* To maximise commercial benefits;
* To focus on the Customer (Buyer)
* To help strengthen the UK economy through effective policy delivery.

The DPS for Cyber Security Services will support these priorities. It offers a route to quality Services provided by suppliers who can offer a range of experience and industry standards.

The DPS is a dynamic commercial model, which suppliers can join via a straightforward selection process. Buyers will be able to access a wider market of suppliers, obtain more choice and achieve better value.

The range of services available via this DPS will help Buyers to protect public assets and comply with regulatory requirements for protecting citizens’ data.

## **1.2 Scope**

This section sets out what CCS and our Buyers want.

The Supplier must only provide the Deliverables for the Filter Categories to which they have been appointed.

For all Filter Categories and/or Deliverables, the Supplier must help Buyers comply with any specific applicable Standards of the Buyer.

There are four Filter Categories available on the DPS:

1. Certified NCSC Services / Non-certified NCSC Services
2. Service Types
3. Accreditations and standards available (in addition to NCSC)
4. Sectors / Experience

**1.3 Service Types**

The Supplier has demonstrated that they can supply Services within at least one of the following Service Types as documented in the DPS Appointment Form associated with their DPS Contract.

|  |  |  |
| --- | --- | --- |
| **Category/ Service type** | | **Service Description/ Example** |
| Consultancy and Advice | GovAssure | Independent assurance review of a government organisations self-assessed return against the Cyber Assessment Framework (CAF) by a provider that meets the minimum security clearance and assurance requirements |
| 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 | 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. |
| Cyber Programme Delivery | Delivering a wide range of activities such as planning, implementing and managing initiatives aimed at improving cyber security within an organisation |
| 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. |
| Red Teaming | Red teaming is an exercise used to test capabilities and is when an authorised individual/ team simulate an attack on your estate utilising physical, technical and social engineering methods. |
| 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. |
| Cyber Incident Response Level 1 | NCSC assured service providing cyber incident response to the UK Central Government, Critical National Infrastructure or operate in the regulated sector |
| Cyber Incident Response Level 2 | NCSC assured service providing cyber incident response to local government bodies, large, medium and small businesses, and charity organisations within the UK |
| Cyber Exercising | NCSC assured service providing table-top or live play incident exercising for UK Central and Regional Government, and medium and large organisations |
| Disaster Recovery | Providing advice and producing disaster recovery plans. |
| Threat Intelligence | Providing advice on cyber threats drawing upon intelligence from appropriate sources. |
| BCDR | Providing advice and strategies to help organisations build resilience and respond to disasters, including research, impact assessment, testing and training. |
| Data Destruction | Secure data removal and IT sanitisation services. | Secure data erasure and disposal of IT media and assets using audited destruction procedures. |
| Encryption Services | IP Crypto | NCSC assured service, supplier must be approved on the **Crypt Key Company Standard Register** and continue to meet the requirements of the Standard. |
| Managed Security Service | CREST Accredited Security Operations Centre (SOC) | Security Operations Centre (SOC) provided by a CREST accredited supplier who has met the necessary discipline requirements. |
| Security Operations Centre (SOC) | Providing a Security Operations Centre (SOC) which can include activities such as monitoring, detecting, analysing and investigating cyber threats. |
| Managed Detection and Response (MDR) | Providing a proactive managed security service which can include threat intelligence, threat hunting, security monitoring, incident analysis and incident response capabilities. |

The Supplier will use the Skills Framework for the Information Age (SFIA) to describe the roles, levels of responsibility and skills to deliver services under the above service categories. The SFIA framework can be found at:<https://www.sfia-online.org/en/framework>

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.

**1.4 Accreditations and Standards:**

|  |
| --- |
| Cyber Essentials Plus |
| Crest/ Tiger/ Cyber/ Other Qualified |
| PCI Assessor |
| Project Management - APM Qualified |
| Project Management - PRINCE Qualified |
| Clearance: Counter Terrorist Check |
| Clearance: Security Check |
| Clearance: Developed Vetting |
| NPPV (Non-Police Personnel Vetting) |
| Defence Assurance Risk Tool (DART) |
| ISO 27001 |

**1.5 Sectors and Experience:**

|  |
| --- |
| **Experience:** |
| Networks |
| Database |
| Internet |
| Cloud |
| Premises |
| Endpoint / applications |
| GDPR |
| Electronic Warfare (EW) |
| India |
| Indo Pacific |
| Africa |
| Middle East/ North Africa (MENA) |
| Cyber Capacity Building |
| Other |
| **Sector:** |
| Chemicals |
| Civil Nuclear Communications |
| Defence |
| Energy |
| Finance |
| Food |
| Government |
| Health |
| Space |
| Transport |
| Water |
| Critical National Infrastructure |
| Other |
| **CNI Emergency Services:**   * Police * Ambulance * Fire Services * Coastguard * Other |

**1.6 What is outside of the scope of the DPS Contract?**

Products and services out of scope of this DPS include but are not limited to:

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

## **Mandatory Requirements:**

**2.1 Quality Standards**

Suppliers shall use a documented quality management system, as part of delivering services under this DPS. The Supplier may be required by a Buyer to comply with specific quality standards set by industry bodies or Government codes of practice.

**2.2 Security Requirements**

The Supplier shall at all times during the DPS Contract Period and during the term of any Order Contract comply with the Buyer’s contracted security requirements. The Supplier will ensure controls and measures are in place to protect data handled, processed or stored as part of delivering the Services in accordance with Clause 14 of the Core Terms.

The Supplier shall comply with the applicable requirements set out in the Cabinet Office’s Security Policy Framework. Information about the framework can be found at:<https://www.gov.uk/government/publications/security-policy-framework>

The Supplier shall ensure that staff has security clearance to a minimum level: Baseline Personnel Security standard (BPSS). Should a Buyer require a higher level of security clearance this will be made clear in the Order Procedure.

**2.3 Environmental Standards**

Where applicable, the Supplier shall ensure that all Electric and Electronic Equipment (EEE) used or disposed of as part of delivery of the Services, complies with Restriction of Hazardous Substances (RoHs), WEEE regulations, or equivalent. Full details can be found via the following links: <http://www.hse.gov.uk/waste/waste-electrical.htm>

**2.4 Complying with future government requirements and standards**

The Supplier shall comply with relevant future Government requirements and standards in accordance with any Government guidance issued during the DPS Contract Period and as developed and updated, from time to time.

**2.5 Staff and Contractors**

Where appropriate the Supplier shall ensure that appropriate roles and grades of staff will be assigned to the Services in accordance with NCSC - defined experience levels, Skills Framework for the Information Age (SFIA), or other equivalent grading structures used by the cyber security industry for personnel providing the Services offered under this DPS.

**2.7 Social Value**

The Supplier shall identify Social Value options which are appropriate to Buyers

at Order Contract award stage in accordance with the Buyer’s requirements communicated as part of their Order Procedure.

The Supplier shall complete annual Corporate Social Responsibility (CSR) assessments upon request from Buyers where specified as part of their Order Contract Obligations.

For more information on Social Value please see the following link:

<https://www.gov.uk/government/publications/social-value-act-introductory-guide>