Contract Reference: PS/23/99

Specification

IT Security Incident Response Service

ITS

**Contract Reference:** PS/23/99

**Framework Title & Reference:** Cyber Security Services 3 RM3764.3

## Date: 01/06/2023 Version: v0.7

November 2022

1. [Introduction 3](#_bookmark0)
2. [Background to the Requirement 3](#_bookmark1)
3. [Procurement Timetable 3](#_bookmark2)
4. [Scope 4](#_bookmark3)
5. [Implementation and Deliverables 4](#_bookmark4)
6. [Specifying Goods and / or Services 4](#_bookmark5)
7. [Quality Assurance Requirements 7](#_bookmark6)
8. [Other Requirements 7](#_bookmark7)
9. [Management and Contract Administration 14](#_bookmark8)
10. [Training / Skills / Knowledge Transfer 14](#_bookmark9)
11. [Documentation 14](#_bookmark10)
12. [Arrangement for End of Contract 14](#_bookmark11)
13. [Response Evaluation 14](#_bookmark12)

Annex 1 18

[Annex 2 19](#_bookmark13)

# Introduction

In accordance with the terms and conditions of Cyber Security Services 3 RM3764.3 the Driver and Vehicle Licensing Agency (DVLA) invites proposals for the following services.

# Background to the Requirement

The DVLA is an Executive Agency of the Department for Transport (DfT), based in Swansea. The DVLA’s primary aims are to facilitate road safety and general law enforcement by maintaining accurate registers of drivers and vehicle keepers and to collect Vehicle Excise Duty (VED).

DVLA’ Information Technology Services (ITS) require a call-off contract for specialised security support in the event of cyber security incidents (including undertaking digital forensic investigation) and high quality trusted relevant Threat Intelligence Alerting.

# Procurement Timetable

The timetable for this procurement is set out in the table below. The timetable may be changed at any time but any changes to the dates will be made in accordance with the Regulations (where applicable).

Suppliers will be informed if changes to the timetable are necessary.

The key dates for this procurement (**Timetable**) are currently anticipated to be as follows:

|  |  |
| --- | --- |
| **Description** | **Date** |
| Invitation to Tender | 18.07.2023 |
| Deadline for Clarification Questions | 5pm 21.07.2023 |
| Deadline for DVLA to respond to  clarification questions | 5pm 25.07.2023 |
| Deadline for submission of tender | 5pm on 28.07.2023 |
| Evaluation of tender | 31.07 – 02.08.23 |
| Proposed intention to award/Decline  letters | 03.08.2023 |
| Standstill | 04.08.23 – 14.08.2023 |
| Issue contract Award letter | 15.08.2023 |
| Contract Start date | 16.09.2023 |

DVLA reserves the right to amend the Timetable. Any changes to the Timetable shall be notified to all suppliers as soon as practicable.

# Scope

ITS require a call-off contract for specialised security support in the event of cyber security incidents (including undertaking digital forensic investigation) and high quality trusted relevant Threat Intelligence Alerting.

The successful supplier must be an organisation which specialises in providing cyber security incident response retainer services and understands cyber threats. They must have the resource capability to provide consultants 24 hours a day 365 days a year, who can deal with technical and non-technical Cyber Security crisis, with the ability to mobilise consultancy within 4 hours.

The supplier must have:

* + Government-run Cyber Incident Response (CIR) certification run by NCSC and CPNI (Centre for the Protection of National Infrastructure).
  + Experience of dealing with sophisticated, targeted attacks against Government networks of national significance.
  + Evidence of working with Government organisations in developing an Incident Response Plan.

# Implementation and Deliverables

The contract term will be 2 years, commencing 16th September 2023.

To ensure the contract runs smoothly the successful supplier must provide an Account Manager who will act as the first point of contact for all enquiries.

Service Review meetings are required as part of this contract, with the frequency to be agreed. Meetings will be held via MS Teams.

# Specifying Goods and / or Services

The details of the requirement are:

* + A call-off contract for up to 90 days of specialist response time for response SLAs and prioritisation, to the standard detailed in Section 6.1.
  + Call-off retainer of 15 days of specialist response time, which will provide initial support while we work with the Supplier should we need to call-off additional days. These 15 days will be deducted from the 90 day call-off and paid up front following contract award, with any additional days called-off during the contract term invoiced at the appropriate time.
  + If the initial 15 days (prepaid) are not used by the end of the contract term they must be converted to consultancy services or training, which should be utilised within 6 months of the end of the contract.
  + Undertake digital forensic investigations in a manner that is forensically sound and meets the requirement for legal admissibility in the event of a court case resulting.
  + Personnel must be suitably cleared for the task they are undertaking and which may vary depending on specific functions (refer to Section 8).
  + Threat Intelligence Alerting service, including monthly, quarterly and adhoc reports as/when required.
  + All support should be provided from the United Kingdom, or where not feasible from locations agreed in advance BEFORE the contract is in place.
  + The Supplier must work with the Business to undertake a minimum of one joint incident response exercise each year.

## Service Level Agreement (SLA) and Key Performance Indicators (KPIs)

The details of the SLA and KPIs applicable to this requirement are outlined below;

The Supplier shall provide the Services so as to meet or exceed the Service Levels set out in this Schedule.

Meeting or exceeding a Service Level indicates that the Supplier is meeting some (but not necessarily all) of its contractual commitments to the Customer with respect to levels of performance.

Service Levels may be added, deleted, or modified and agreed by both parties at any time during the Term, in accordance with the change control procedure in the call off agreement. For the avoidance of doubt, the Supplier shall not withhold or delay its consent to any requested changes to the Service Levels that are required to achieve a fair, accurate and consistent measurement of the Supplier’s performance in delivering the Services.

The Supplier shall use appropriate tools in order to measure and report the levels of performance of the Services that are subject to the Service Levels. Such measurement shall permit reporting that is detailed enough to verify compliance with the Service Levels which can reviewed in service review meetings.

## Service Response

|  |  |  |
| --- | --- | --- |
| **Service** | **Description** | **SLA Target** |
| Account Management | Regular Service Review meetings to be held with DVLA Business Area | Fortnightly |
| Support | In hours support to be provided from within the UK. | Core UK working hours |
| Support | IR personnel on standby | 24/7 365 |

|  |  |  |
| --- | --- | --- |
| Support | Access to dedicated telephone line | 24/7 365 |
| Service Response | Telephone | Within 1 hour |
| Service Response | Remote Incident Support | Within 12 hours |
| Service Response | Onsite Support (T&S including) | Within 12 hours |
| Service Response | Triage time included | Within 2 hours |
|  | First Responder training (remote) | 8 delegates |
| Threat Intelligence Alerting service | Monthly & Quarterly Reports | Dates to be agreed |
| Threat Intelligence Alerting service | Ad hoc Reports | Within 48 hours |

## Transparency/Publication of Key Performance Indicators (KPIs)

Not applicable

## Social Value Considerations

Not applicable

## Modern Slavery Considerations

Any requirements of the Modern Slavery Act 2015 or Procurement Policy Note (PPN) 05/19, which are appropriate to your requirement, should also be set out here.

## Prompt Payment Considerations

The Government understands the importance of prompt, fair and effective payment in all businesses. Being paid promptly for work done ensures businesses have a healthy cash flow. Procurement Policy Note [PPN 08/21](https://www.gov.uk/government/publications/procurement-policy-note-0821) sets out how payment approaches can be taken into account in the procurement of major Government contracts and this requirement falls into scope of the PPN. Bidders are required to confirm that they still meet the prompt payment requirements as set out in Framework Cyber Security Services 3 RM3764.3

## Supply Chain Visibility

The Government wants to level the playing field and increase the visibility of supply chain opportunities to assist suppliers, including SMEs, in bidding for work in its supply chains. [Procurement Policy Note (PPN) 01/18](https://www.gov.uk/government/publications/procurement-policy-note-0118-supply-chain-visibility) sets out the requirement for successful suppliers of

in-scope procurements to advertise subcontracting opportunities and report on how much they spend with Small/Medium Enterprises (SME) and Voluntary, Community and Social Enterprises (VCSE). This requirement is in scope of this PPN and requires the successful prime supplier(s) to:

1. advertise on [Contracts Finder](https://www.gov.uk/contracts-finder), subcontract opportunities arising from that contract above a minimum subcontract threshold of £25,000; and
2. separately, report on how much they spend on subcontracting, and separately how much they spend directly with SME or VCSE organisations in the delivery of the original contract

The contracted supplier will be required to fulfil the reporting requirements as set out in the PPN and the Terms and Conditions of this requirement.

## Sourcing Playbook Considerations

Not applicable

## Net Zero Carbon Reduction Plans

Not applicable

# Quality Assurance Requirements

The contracted supplier must secure Cyber Essentials certification prior to the contract commencement, refer to 8.2.

# Other Requirements

## Information Assurance Removable Media

Suppliers should note that removable media is not permitted in the delivery of this Contract. Where there is a requirement for Supplier Staff to take data off site in electronic format, the DVLA will consider if it is appropriate to supply an encrypted hard drive.

## Security Clearance Level 1

Suppliers are required to acknowledge in their response that any Supplier Staff that will have access to the DVLA site for meetings and similar (but have no access to the DVLA systems), must be supervised at all times by DVLA staff.

## Level 2

Suppliers are required to confirm in their response that any Supplier Staff that will be accessing the DVLA Site to provide routine maintenance or have access to the DVLA site and DVLA systems have Baseline Personnel Security Standard clearance (BPSS). The BPSS comprises verification of the following four main elements:

1. Identity;
2. Employment History (past 3 years);
3. Nationality and Immigration Status;
4. Criminal Record Check (unspent convictions only).

The aim of the Baseline Standard verification process is to provide an appropriate level of assurance as to the trustworthiness, integrity and proper reliability of prospective staff. Suppliers are required to provide evidence of relevant Supplier Staff clearance in their response.

## Processing Personal Data and Data

Please note that the successful supplier as part of the contract agrees to comply with all applicable requirements of UK Data Protection Legislation (including UK GDPR) and all applicable Law about the processing of personal data and privacy.

## Processing of Government Data

This contract will require the successful supplier to process Government data on DVLA’s behalf. The successful supplier will be required to complete a Statement of Assurance Questionnaire (SoAQ) prior to formal contract award and before any processing of data commences in relation to this contract, to satisfy DVLA that its data will be appropriately protected. The SoAQ is included as part of the ITQ as an Appendix. The purpose of the Questionnaire is to assess the maturity of policies, systems and controls associated with the handling of our data. The Questionnaire was developed for use throughout the Government supply chain and is based on ISO27001 criteria and aligned to the HMG Security Policy Framework.

Suppliers are required to confirm their understanding and acceptance of the requirement to complete and return the Questionnaire during the Standstill Period.

The completed Questionnaire will be assessed by our Information Assurance Group and DVLA will work with the successful supplier to address any information aspects requiring improvement.

The HMG Security Policy Framework requires Departments to conduct an annual compliance review of third-party suppliers. The Questionnaire will therefore need to be completed annually throughout the term of the contract in order to assess ongoing compliance. DVLA may also audit suppliers to validate the responses and evidence provided in the Questionnaire.

## Processing Personal Data

Please note that the successful tenderer as part of the contract agrees to comply with all applicable requirements of UK Data Protection Legislation (including UK GDPR) and all applicable Law about the processing of personal data and privacy.

## Schedule of Processing, Personal Data and Data

The processing of personal data has been identified as part of this requirement. Please refer to the Terms and Conditions of this contract for full details of the instructions to be followed when processing data.

## Information Supply Chain

Suppliers are required to confirm how DVLA Data will be securely managed at each stage of the Information Supply Chain. This applies to both suppliers and subcontractors. Retention schedules will need to be defined and agreed prior to award of contract.

## Offshoring of Government Data

Government policy is that data it holds should be protected appropriately regardless of location.

Offshoring is defined as “Any arrangement where the performance of any part of the services or a solution under a contract may occur outside the UK for domestic (UK) consumption.”

When offshoring is described, the focus is typically on the physical location where data is hosted (such as where are the data centres located). Whilst physical location of data is a critical part of the offshoring question, it is important to understand how and where data might be logically accessed. Administrators or technical support staff may be located anywhere in the world, with logical access to data.

Suppliers must indicate in their response whether any DVLA data supplied as part of the contract, would be offshored. If so, suppliers must confirm the location(s) including the location of any business continuity, disaster recovery and technical support staff.

All Central Government Departments and Agencies are required to seek approval for any proposed offshoring activity, which ensures that information held offshore is appropriately managed and that pan-government risks are identified, tracked and managed, where appropriate.

In the event that the successful supplier proposes to offshore any DVLA Data as part of the contract, they would be required to provide details about the processing to be carried out offshore, the privacy risks and the security controls in place to protect the data. If the intention is to store the information in a cloud environment outside the UK, the successful supplier will also need to confirm the extent to which the environment complies with the cloud security principles. This information would be used to submit the offshoring proposal for approval.

Any request to offshore must receive clearance prior to the commencement of any data processing activity.

## Redundant Equipment

Any redundant equipment that will have captured any DVLA sourced data must be disposed of securely on the DVLA Site.

## Cyber Security

The Government has developed Cyber Essentials, in consultation with industry, to mitigate the risk from common internet-based threats.

It will be mandatory for new Central Government contracts, which feature characteristics involving the handling of personal data and ICT systems designed to store or process data at the OFFICIAL level of the Government Security Classifications scheme (link below), to comply with Cyber Essentials.

<https://www.gov.uk/government/publications/government-security-classifications>

All potential suppliers for Central Government contracts, featuring the above characteristics, should make themselves aware of Cyber Essentials and the requirements for the appropriate level of certification. The link below to the Gov.uk website provides further information:

<https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

As this requirement features the above characteristics, you are required to demonstrate in your response that:

* + - Your organisation has Cyber Essentials certification; **or**
    - Your organisation will be able to secure Cyber Essentials prior to commencement of the required services/deliverables; **or**
    - Your organisation has other evidence to support that you have appropriate technical and organisational measures to mitigate the risk from common internet- based threats in respect to the following five technical areas:
      * Boundary firewalls and internet gateways
      * Secure configuration
      * Access control
      * Malware protection
      * Patch management

The successful supplier will be required to provide evidence of Cyber Essentials certification ‘or equivalent’ (i.e. demonstrate they meet the five technical areas the Cyber Essentials Scheme covers) prior to commencement of the required services/deliverables. This will be through the completion of the Statement of Assurance Questionnaire (SoAQ).

The successful supplier will be required to secure and provide evidence of Cyber Essentials re-certification ‘or equivalent’ (i.e. demonstrate they meet the five technical areas) on an annual basis.

## Further information regarding the certification process can be found here:

<https://www.ncsc.gov.uk/cyberessentials/overview>

## Data Sharing

DVLA’s Contract Owner will work with the successful supplier to implement any information sharing or data sharing procedures and associated DVLA requirements that may be needed at any point during the lifecycle of the contract.

Information or data sharing procedures will need to be formally assessed and approved by DVLA through the Data Sharing Clearance Process, managed by the Information Assurance & Governance team (IAG).

The Supplier will submit any requirements for information / data sharing via the Contract Owner to the DVLA who will consider the changes through this Data Sharing Clearance process. Any proposals shall be considered and if approved an implementation plan will be formally offered to and accepted by both the DVLA and the Supplier before commencement.

This approvals process is designed to assess and identify additional measures and safeguards that may be required to protect data to those already stated in this specification document.

## Sustainability

DVLA is committed to reducing any negative impacts produced by our activities, products and services. This aligns to the Greening Government Commitments which states we must: “Continue to buy more sustainable and efficient products and services with the aim of achieving the best long-term, overall value for money for society.”

DVLA is certified to ISO 14001:2015 and more information is available in our Environmental Policy at:

<https://www.gov.uk/government/publications/dvlas-environmental-policy>

The Supplier shall comply with DVLA’s Environmental Policy.

Where appropriate, the Supplier shall assist DVLA in achieving its Greening Government Commitments as detailed on [Greening Government Commitments 2021 to](https://www.gov.uk/government/publications/greening-government-commitments-2021-to-2025) [2025 - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/greening-government-commitments-2021-to-2025) i.e. Reduce CO₂ emissions through energy consumption and travel, reduce water consumption and waste produced.

If requested, the Supplier shall be able to provide data on carbon emissions related to the services being supplied to aid with scope 3 emission calculations.

If available, the Supplier shall provide a copy of their sustainability or environmental policy.

The Supplier shall promote resource efficiency and waste avoidance, to reduce waste arising and consumption of natural resources. Any waste shall be disposed of correctly and in accordance with the waste hierarchy and duty of care, and any applicable legislation.

The Supplier shall continually aim to travel sustainably when attending a DVLA site.

The Supplier shall be committed to reducing their carbon emissions in line with per year.

The Supplier shall ensure that any activities conform to overarching principles in the [Greening Government ICT and digital services strategy 2020-2025](https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025). Namely the

Government’s vision to be a global leader in sustainable ICT. The Supplier must confirm their understanding and acceptance of the strategy.

## Health and Safety

DVLA has an Occupational Health and Safety Management System that is certificated to ISO45001. Further information on our Health & Safety Policy, is available on request.

All Supplier Staff working in the DVLA on any of our premises must fully comply with relevant health and safety legislation, together with health, safety and welfare policy and management arrangements applied by the DVLA. If appropriate, these issues must be addressed at or before the award of the contract and may form part of the procurement process. Where requested, Suppliers will be required to provide copies of their health and safety policy statement, risk assessments and method statements, clearly identifying any safety implications that their activities may have and how these will be managed. Contract management staff are responsible for checking health and safety information provided by Suppliers and passing relevant information to local line management and staff. Supplier’s safety performance will be monitored and checked as part of normal contract management.

Suppliers should:

* + - Have an appointed competent person responsible for H&S, details to be made available to DVLA on request
    - Have emergency arrangements and plans for their goods/product/service, and observe DVLA’s arrangements whilst on site, or through the course of the business or contract
    - Have adequate provision for your own first aid when on site
    - Have an accident reporting and recording process for all near miss, accidents/incidents, or violent and aggressive behaviours. Any incident on DVLA site should be reported immediately to the DVLA’s Health and Safety Team
    - Communicate with DVLA on any health and safety matter or issue in relation to the contract/product/supply of goods or service, notifying DVLA of any Health and Safety hazard, which may arise in connection with its supply of goods, products, or services
    - Indemnify DVLA in the instance where failure of the company’s product/service, acts or omissions, with regards to health and safety, results in an economic penalty, time delay, issue, accident/incident or claim against the DVLA
    - Have suitable and sufficient insurance cover for all business/products/services supplied/that are provided to DVLA
    - Have documented, suitable and sufficient, risk assessments and method statements, covering all significant activities and deliveries of products, goods and services. Copies to be made available to DVLA on request
    - Provide suitable and sufficient health and safety training, information and instruction for all its employees/contractors/subcontractors. Records to be made available on request
    - Engage with DVLA’s Security/Estates Management Group to arrange access to all DVLA premises/buildings
    - Comply with all vehicle and driver legal requirements and DVLA policies whilst driving on premises or conducting business for DVLA

## Estates

Not applicable

## Diversity and Inclusion

The Public Sector Equality Duty (PSED) is a legal requirement under the Equality Act 2010. The Equality Duty ensures that all public bodies play their part in making society fairer by tackling discrimination and providing equality of opportunity for all. It ensures that public bodies consider the needs of all individuals in their day-to-day work – in shaping policy, in delivering services, and in relation to their own employees. DVLA is committed to encouraging equality, diversity and inclusion within our workforce and against unlawful discrimination of employees, customers and the public. We promote dignity and respect for all and will not tolerate bullying, harassment or discrimination by staff, customers or partners we work with. Everyone working for us and with us, as partners in delivering our services, has a personal responsibility for implementing and promoting these policy principles in their day- to-day transactions with customers and our staff.

A full copy of our Equality, Diversity and Inclusion Policy is available on request from the DVLA.

## Business Continuity

Suppliers shall have robust Business Continuity and Disaster Recovery Plans which align to a code of practice such as ISO22301. Suppliers must supply the contents of these plans to the Agency.

The successful supplier will test their business continuity arrangements no less than once per annum and shall inform the Agency when such tests or exercises are scheduled. Outcomes of these tests or exercises must be made available to the Agency in writing upon request.

Suppliers will notify DVLA in writing within twenty-four (24) hours of any activation of the business continuity plan, in relation to the services provided to DVLA.

## Procurement Fraud

The DVLA adopts a zero tolerance approach to procurement fraud and bribery. Please read the DfT Counter Fraud, Bribery, Corruption and Ethical Procurement Statement in **Appendix A.** DVLA expect you to adhere to the information contained within the appendix.

## Use of DVLA Brands, Logos and Trademarks

The DVLA does not grant the successful Supplier licence to use any of the DVLA’s brands, logos or trademarks except for use in communications or official contract documentation, which is exchanged between the DVLA and the successful Supplier as part of their fulfilment of the Contract.

Approval for any further specific use of the DVLA’s brands, logos or trademarks must be requested and obtained in writing from the DVLA.

## Welsh Language Scheme Requirements

Not applicable

## Delivery Instructions – Goods

Not applicable

# Management and Contract Administration

## Subcontracting to Small and Medium Enterprises (SMEs):

DVLA is committed to removing barriers to SME participation in its contracts, and would like to also actively encourage its larger suppliers to make their subcontracts accessible to smaller companies and implement SME-friendly policies in their supply-chains (see the Gov.Uk [website](https://www.gov.uk/government/publications/department-for-transport-actions-for-improving-business-opportunities-for-small-and-medium-enterprises) for further information).

To help us measure the volume of business we do with SMEs, our Form of Tender document asks about the size of your own organisation and those in your supply chain.

If you tell us you are likely to subcontract to SMEs, and are awarded this contract, we will send you a short questionnaire asking for further information. This data will help us contribute towards Government targets on the use of SMEs. We may also publish success stories and examples of good practice.

# Training / Skills / Knowledge Transfer

XXXXXX “redacted under FOIA section No 43 – Commercial Interests”

# Documentation

DVLA Invoicing Procedures are detailed in **Appendix B** - DVLA Invoicing Procedures.

# Arrangement for End of Contract

The Supplier shall fully cooperate with the DVLA to ensure a fair and transparent re- tendering process for this contract. This may require the Supplier to demonstrate separation between teams occupied on the existing Contract and those involved in tendering for the replacement contract to prevent actual (or perceived) conflicts of interest arising.

# Response Evaluation

The evaluation will comprise of the following elements:

1. an evaluation of mandatory requirements, if applicable. These will be assessed on a pass/fail basis. Responses that fail any of the mandatory requirements may be disqualified from further consideration
2. an evaluation of the response based on the quality criteria
3. an evaluation of the prices submitted

Selection will be based on the evaluation criteria, which demonstrates a high degree of overall value for money, competence, credibility and ability to deliver.

Your response will be evaluated using the following weightings **and** the criteria weightings set out at Annex 1 to obtain the optimal balance of quality and cost.

## Mandatory Requirements (if applicable)

Annex 1 provides details of any elements/criteria considered as critical to the requirement. These are criteria, which will be evaluated on a pass/fail basis. A fail may result in the response being excluded from further evaluation.

## Quality Criteria:

Annex 1 provides details of the quality criteria on which responses will be evaluated. This will list the primary criteria along with the allocated percentage weighting and a description of the specific requirement. The overall percentage allocated for the quality criteria is outlined in the table “Overall Weighting Allocation” and the method used to allocate scores is outlined below.

## Minimum threshold to pass for final evaluation

For **Technical Criteria 1** - Experience of dealing with sophisticated, targeted attacks against Government networks of national significance.

**Technical Criteria 2** - Evidence of working with Government organisations in developing an Incident Response Plan.

**Technical Criteria 3 –** The supplier must provide detailed information on support location(s) based in and outside UK. If support is outside the UK then further evidence will need to be provided whilst confirming the process carried out for offshoring.

As these questions are deemed critical for this requirement a minimum threshold of 60 points awarded must be achieved in order to be deemed a compliant bid.

## Quality Criteria Scoring Methodology:

The scoring methodology used to assess and allocate scores to each criteria are included in the table below.

|  |  |
| --- | --- |
| **Points awarded** | **Description** |
| 100 | Fully meets/evidence provided that demonstrates the requirement can be met |
| 60 | Minor concerns/issues that the requirement can be met |
| 30 | Major concerns/issues that the requirement can be met |
| 0 | Does not meet the requirement, not addressed or no evidence provided |

Based on the allocated score, a percentage will be calculated against each element using on the following calculation:

(Allocated Score Maximum Score)



X Weighting

For example, “Quality Element 1” can be allocated a score between 0 and 100 but carries a weighting of 10%. Supplier A is given a score of 60 for this element so receives a score of (60/100 x 10) = 6%. The scores for each element will then be added together to calculate the overall quality criteria score.

## Financial / Price Criteria

Evaluation of the prices submitted will be performed separately by a Commercial Finance Accountant and details will not be made available to the Quality Evaluation Panel. This is to ensure fairness and avoid any subconscious influence of a lower price on the quality scoring. The overall percentage weighting allocated for the Financial/Price Criteria is outlined in the table “Overall Weighting Allocation”.

## Financial / Price Criteria Scoring Methodology:

A Percentage Scoring Methodology will be used to evaluate all proposals for this requirement. This methodology is based on the following principles:

The lowest quoted price will be awarded the maximum score available. Each subsequent responses will be baselined to this score and will be awarded a percentage of the maximum score available. The calculation used is as follows:

(Lowest Quoted Price Price Quoted per Supplier)



X Maximum Score Available (i.e. Weighting)

For example, if the Financial/Price weighting allocation is 40%, the maximum score available is 40. Supplier A submits the lowest price of £100,000 and Supplier B submits

a price of £180,000. Based on the above calculation Supplier A and B will receive the scores shown below:

Supplier A = 100k/100k x 40 = 40% Supplier B = 100k/180k x 40 = 22.22%

## Overall Weighting Allocation

|  |  |
| --- | --- |
| **Evaluation Criteria** | **Weighting** |
| **Technical Criteria** | 75% |
| **Financial / Price Criteria** | 25% |
| **Total** | 100% |

## Calculation of Overall Score:

The allocated score for the quality/Technical and Financial/Price Factor score to calculate the overall score for each tender (out of a max available 100%). The tender with the highest overall score will be deemed as successful.

1. **Points of Contact**

|  |  |  |
| --- | --- | --- |
| **Commercial Advisor** | Name | XXXXXX “redacted under FOIA section No 40 – Personal Information” |
| e-mail | XXXXXX “redacted under FOIA section No 40 – Personal Information” |
| **Business Area Contact ITS** | Name | XXXXXX “redacted under FOIA section No 40 – Personal Information” |
| Tel | XXXXXX “redacted under FOIA section No 40 – Personal Information” |
| e-mail | XXXXXX “redacted under FOIA section No 40 – Personal Information” |

## All queries/questions should be sent to the Commercial Advisor

**Annex 1 Evaluation Criteria**

## Mandatory Criteria

Responses that fail any of the mandatory requirements may be disqualified from further consideration

|  |  |  |
| --- | --- | --- |
| **Mandatory Criteria** | **Mandatory Criteria Description** | **Pass/Fail** |
| **Criteria 1** | The Supplier must have capability to provide consultants 24 hours a day 365 days a year, who can deal with technical and non-technical Cyber Security crisis, with the ability to mobilise consultancy within 4 hours. |  |

## Scored Quality Criteria

## Minimum threshold to pass for final evaluation

As these questions are deemed critical for this requirement a minimum threshold of 60 points awarded must be achieved in order to be deemed a compliant bid.

|  |  |  |  |
| --- | --- | --- | --- |
| **Primary Scored Criteria** | **Primary Scored Criteria Weighting (%)** | **Scored Sub-criteria Description** | **Individual Scored Sub - Criteria**  **Weighting (%)** |
| Technical Criteria | **75%** | Experience of dealing with sophisticated, targeted attacks against Government networks of national significance. **Max 500 words** | 30% |
| Evidence of working with Government organisations in developing an Incident Response Plan. **Max 500 words** | 30% |
| The supplier must provide detailed information on support location(s) based in and outside UK. If support is outside the UK then further evidence will need to be provided as part of the evaluation process, whilst confirming the process carried out for offshoring.  **Max 500 words** | 40% |
|  | **Total = 75%** |  | |

## Financial/Pricing Criteria

|  |  |  |
| --- | --- | --- |
| **Primary**  **Financial/Pricing Criteria** | **Financial/Pricing Weighting (%)** | **Description** |
| **Pricing Requirements** | **25%** | **Refer to the Pricing Schedule** |
|  | **Total = 100%** |  |

## Appendix A



DfT Counter Fraud Bribery Corruption an

## Appendix B



Invoicing Procedures.docx