

**Freedom of Information request reference number:** 9164.1

**Date of response:** 18/11/2024

**Request:**

I would like to request the following under the Freedom of Information Act, to be sent to me electronically: 1) A copy of the LFC cyber-defence system contract which replaced the previous contract in July 2023, and any other relevant documents related to the procurement 2) Details of the procurement process for the above contract 3) A copy of the most up-to-date version of your Cyber security policy

**Response:**

Further to your request, please see below for redacted copies of the documents. The procurement process is included in the document *7108 IPP Cyber Defence System*. Personal information has been removed from the contract under [section 40 of the FOIA – Personal Information](#).

A copy of the recent Cyber security policy is available online so is exempt from release under [section 21 of the FOIA – information reasonably accessible by other means](#). A copy of the policy can be found here: <https://www.london-fire.gov.uk/media/5814/lfc-0514x-cyber-security-policy-d.pdf>.

We have dealt with your request under the Freedom of Information Act 2000. For more information about this process please see the guidance we publish about making a request on our website: <https://www.london-fire.gov.uk/about-us/transparency/request-information-from-us/>



**The London ICT Framework / London Procurement Partnership**

***London Fire Darktrace***

***London Fire and Emergency Planning Agency***

|                  |            |
|------------------|------------|
| CCN No:          | LFBCCN0024 |
| Version:         | 1.1        |
| Author:          | [Redacted] |
| Document Status: | Issue      |
| Issue Date:      | 27/06/2023 |

E-signed 2023-06-28 01:34PM GMT+1  
[Redacted]@london-fire.gov.uk



E-signed 2023-06-28 01:50PM GMT+1  
[Redacted]@bt.com

BT



Document Integrity Verified

[Redacted]



### Confidentiality Statement

The information set out in this proposal that is marked 'In Confidence' may include, but not be limited to, information such as licensed prices, design documents, plans and any information relating to BT's customers. This information is communicated in confidence and disclosure of it to any person without BT's consent will be treated as a breach of confidentiality.

Furthermore, the disclosure of information that is commercially confidential to BT may, or may be likely to, prejudice BT's commercial interests. We believe that such commercially confidential information will be exempt from the duty to confirm or deny, and from disclosure, under the Freedom of Information Act 2000.

Many of the products, services, and company names referred to in this document are trademarks or registered trademarks.

They are hereby acknowledged.

All transactions are subject to the appropriate BT Standard Terms and Conditions.

Copyright

© British Telecommunications plc, 2023

Registered office: 1 Braham Street, London E1 8BB

### Freedom of Information Act 2000

For the purpose of the Freedom of Information Act 2000, design information contained in this section (excluding any published information on any components or products specified in the design or any other information which is published or becomes known legitimately from a source other than BT) is provided **IN CONFIDENCE**.

### Document Details

This document is subject to change-controlled release.

|                      |   |            |                   |
|----------------------|---|------------|-------------------|
| Document Title       | London Fire Darktrace                     |            |                   |
| Customer             | London Fire and Emergency Planning Agency |            |                   |
| CCN Number           | LFBCCN0024                                | Version    | 1.1               |
| Document Status      | Issue                                     | Issue Date | 27/06/2023        |
| Author               | [REDACTED]                                | Job Title  | SRM Professional  |
| Phone Number         | [REDACTED]                                | E-Mail     | [REDACTED]@bt.com |
| CCN Template version | 1.10a                                     |            |                   |

Table 1 - Document Details

[REDACTED]  
E-signed 2023-06-28 01:34PM GMT+1  
[REDACTED]@london-fire.gov.uk



[REDACTED]  
E-signed 2023-06-28 01:50PM GMT+1  
[REDACTED]@bt.com  
BT



**Document Approval for Release**

The release of this document to the customer is subject to approval by all applicable Service Provider stakeholders implicated in the scope of this Contract Change. All approvers in the table below will need to approve the document before the overall status can be marked as "Approved".

| Approver Role                            | Required?                           | Approved                            |
|--|-------------------------------------|-------------------------------------|
| Solution / Technical Compliance          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Solution / Project Delivery              | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Client Service Delivery / CSM            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Framework Commercial / Contract Director | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Document Status / Approval for Release:  | Issue                               |                                     |

Table 2 – Approval of Document for Release

**Version History**

The latest approved version of this document supersedes all other versions. Upon receipt of the latest approved version all other versions should be destroyed unless it is specifically stated that previous version(s) are to remain extant. If in any doubt, please contact the document Author.

| Version | Date Completed | Updated By: | Change Summary  |
|---------|----------------|-------------|---|
| 0.1     | 08/06/2023     | [Redacted]  | Initial Draft Completed   |
| 0.1     | 12/06/2023     | [Redacted]  | Peer Review   |
| 0.2     | 14/06/2023     | [Redacted]  | Updated   |
| 0.2     | 14/06/2023     | [Redacted]  | Framework Approved  |
| 1.0     | 14/06/2023     | [Redacted]  | Issue   |
| 1.1     | 27/06/2023     | [Redacted]  | Re Issue with revised attachments, minor amendments to scope and responsibilities |

Table 3 - Version Control

 [Redacted]  
 E-signed 2023-06-28 01:34PM GMT+1  
 [Redacted]@london-fire.gov.uk
 

 [Redacted]  
 E-signed 2023-06-28 01:50PM GMT+1  
 [Redacted]@bt.com  
 BT
 

CONTENTS

**1 PART A - REQUIREMENTS OF CHANGE..... 5**

1.1 DETAILS OF PROPOSED CONTRACT CHANGE.....5

1.2 SERVICES AMENDED BY CHANGE.....7

1.3 BENEFITS OF CHANGE...../

1.4 IMPACT OF NON-IMPLEMENTATION...../

1.5 SPECIFIC CUSTOMER NOTES.....7

**2 PART B – PROPOSED SOLUTION ..... 8**

2.1 REFERENCE MATERIALS .....8

2.2 SOLUTION OVERVIEW .....8

2.3 DELIVERABLES .....12

2.3.1 Service Provider Responsibilities .....12

2.3.2 Customer Responsibilities .....12

2.3.3 Third-Party Responsibilities.....12

2.3.4 Notes.....13

2.3.5 Risks.....13

2.3.6 Assumptions .....13

2.3.7 Issues.....13

2.3.8 Dependencies.....13

2.3.9 Out of Scope .....13

2.4 ADDITIONAL INFORMATION .....14

2.4.1 Project Plan.....14

2.4.2 Service Transition.....14

2.4.3 Timescales.....14

2.4.4 Proposed Changes to Contract Terms.....14

2.4.5 Other Relevant Information / Related CCNs.....14

2.5 IMPACT ON CHANGES .....15

2.5.1 Terms.....16

2.6 ISSUANCE OF CCN.....18

**3 PART C – AUTHORITY TO PROCEED ..... 19**

**APPENDIX A ADDITIONAL NOTES FOR DOCUMENT COMPLETION ..... 20**

3.1 ADDITIONAL NOTES FOR COMPLETION OF PART A.....20

3.2 ADDITIONAL NOTES FOR COMPLETION OF PART B.....21

E-signed 2023-06-28 01:34PM GMT+1  
@london-fire.gov.uk



E-signed 2023-06-28 01:50PM GMT+1  
@bt.com



## 1 Part A - Requirements of Change

| London ICT Framework – Change Control Request Form  |                       |                             |                              |
|---|-----------------------|-----------------------------|------------------------------|
| Request Title:  | London Fire Darktrace |                             |                              |
| <b>Customer</b>   |                       |                             |                              |
| Customer Organisation:  | London Fire Brigade   |                             |                              |
| <b>Requestor</b>  |                       |                             |                              |
| Request Originator / Owner:   | [REDACTED]            |                             |                              |
| Requestor Department:   | CIO                   |                             |                              |
| Contact Number:   | [REDACTED]            | Email address:              | [REDACTED]@londonfire.gov.uk |
| <b>Sponsor</b>  |                       |                             |                              |
| Request Sponsor:  | [REDACTED]            |                             |                              |
| Contact Number:   | [REDACTED]            | Email address:              | [REDACTED]@londonfire.gov.uk |
| <b>Request Details</b>  |                       |                             |                              |
| Request Version: <i>increment! this if Part A changes and has been agreed with customer</i> |                       |                             | 1.0                          |
| Business Unit / BT Account Name:  | London Fire Brigade   | Cost Centre & Account Code: |                              |
| Customer Budget Holder:   | [REDACTED]            | Lot Number                  | 4                            |
| Date Request Submitted:   | 08/06/2023            | Date Response Required By:  | ASAP                         |

### 1.1 Details of Proposed Contract Change

London Fire Brigade would like to use the Darktrace cyber threat detection and defence system.

What are the requirements of the Contract Change –

1. The solution must feature fully autonomous machine learning of standard network device and user activity and be adaptive to normal organisational business, and capable of recognising and proactively blocking anomalous network activity.
2. The solution must have the capability of base lining a network environment in real time without prior knowledge of the environment and support update to the new normal.
3. The solution must be capable of learning the pattern of life for every network, device and user, correlating this information to spot subtle deviations and lateral movement that indicate in progress threats.

E-signed 2023-06-28 01:34PM GMT+1  
[REDACTED]@london-fire.gov.uk

E-signed 2023-06-28 01:50PM GMT+1  
[REDACTED]@bt.com

BT

4. The supplier must state how they will work with the Brigade post implementation, to fine tune the system so that "white noise" and / or "false positives" are reduced to an absolute minimum.
5. The solution must detect and rapidly provide automated, intelligent responses to successfully block cyber-attacks (including APIs and any cyber threat), malware (including zero day attacks and self-encrypting malware) and insider threats.
6. The solution should not rely on rules or signatures, but rather artificial intelligence (AI), heuristics and unsupervised machine learning to accurately detect true threats including threats not detected by traditional SIEM tools.
7. The solution should be able to intelligently auto classify and prioritise threats, supporting workflow and collaboration.
8. The solution must provide 100% network visibility in real time.
9. The solution should be able to model and spot threats emerging from IOT devices.
10. The solution must be able to spot attacks at any point in their life cycle.
11. The solution should be able to graphically display network events and have a user interface that is not only suitable for analysts but information security teams.
12. The solution must be able to accurately detect and block true anomalies for any environment it is deployed onto.
13. The solution must be intelligent enough to automatically filter out false positives with great accuracy.
14. The solution should also be able to self-configure and work automatically on any network.
15. The solution should be passive (AP, SPAN, or NetFlow).
16. Alerting must be able to be outputted to email, SMS and SIEM tools.

[Redacted]  
E-signed 2023-06-28 01:34PM GMT+1  
[Redacted]@london-fire.gov.uk

[Redacted]  
E-signed 2023-06-28 01:50PM GMT+1  
[Redacted]@bt.com

BT

## 1.2 Services Amended by Change

N/A

## 1.3 Benefits of Change

London Fire Brigade at device and user level will be able to monitor, detect in real time and rapidly respond to abnormal network behaviour as well as threats such as malware and advanced persistence threat (APT).

## 1.4 Impact of Non-Implementation

London Fire Brigade will be vulnerable to cyber security threats.

## 1.5 Specific Customer Notes

N/A

E-signed 2023-06-28 01:34PM GMT+1  
@london-fire.gov.uk

E-signed 2023-06-28 01:50PM GMT+1  
@bt.com

BT



## 2 Part B – Proposed Solution

[Redacted]

E-signed 2023-06-28 01:34PM GMT+1  
[Redacted]@london-fire.gov.uk



[Redacted]

E-signed 2023-06-28 01:50PM GMT+1  
[Redacted]@bt.com  
BT



### 3 Part C – Authority to Proceed

|  |                               |
|--|-------------------------------|
| <b>Change Control Note</b>   | <b>CCN Number: LFBCCN0024</b> |
| <b>Part C: Authority to Proceed</b>  |                               |
| Approval for implementation of this CCN as submitted in Part A, in accordance with Part B. Please Select from the below: |                               |
| Please Choose an item.   |                               |

| <b>Originator:</b> | <b>Sponsor:</b>  | <b>Service Provider Representative:</b>                      |
|--------------------|------------------|--|
| <b>Signature</b>   | <b>Signature</b> | <b>Signature</b>   |
| <b>Name</b>        | <b>Name</b>      | <b>Name</b><br>[Redacted]                                    |
| <b>Title</b>       | <b>Title</b>     | <b>Organisation and Title</b><br><br>BT<br>Contract Director |
| <b>Date</b>        | <b>Date</b>      | <b>Date</b><br>14/06/2023                                    |

[Redacted]  
E-signed 2023-06-28 01:34PM GMT+1  
[Redacted]@london-fire.gov.uk

[Redacted]  
E-signed 2023-06-28 01:50PM GMT+1  
[Redacted]@bt.com  
BT

## Appendix A Additional Notes for Document Completion

### 3.1 Additional Notes for Completion of Part A

|                               |   |
|-------------------------------|---|
| <b>Sponsor</b>                | Each Party's Representative is responsible for sponsoring a CCN proposed by a Party.  |
| <b>Customer Business Unit</b> | This is the title of the business unit of the Customer contact with whom the Service Provider has been liaising to create the CCN.  |
| <b>Urgent Change?</b>         | <p>The default priority for a Contract Change is normal.</p> <p>An urgent Contract Change must satisfy one / all the following criteria:</p> <p>There will be a high risk impact on the existing Contract and/or Services within five (5) Business Days if a Contract Change is not initiated;</p> <p>The business impact of not initiating the change quickly is high.</p> |

[Redacted]  
E-signed 2023-06-28 01:34PM GMT+1  
[Redacted]@london-fire.gov.uk

[Redacted]  
E-signed 2023-06-28 01:50PM GMT+1  
[Redacted]@bt.com

BT

### 3.2 Additional Notes for Completion of Part B

A checklist of points to consider when completing CCN Part B is as follows:

| No. | Consideration  | Check - Y / N   |
|-----|--|-----------------|
| 1   | Assessment of the impact (including benefits) on the Services and Services Levels. | Choose an item. |
| 2   | Assessment of the impact on the risk profile of the Services and/or the Contract.  | Choose an item. |
| 3   | Any changes to Sub-contracting arrangements required.                              | Choose an item. |

The specific points to check in relation to the Charges (in accordance with the Charges) are as follows:

| No. | Consideration  | Check - Y / N   |
|-----|--|-----------------|
| 4   | Where a reduction in Charges is being proposed, an analysis of the cost reductions that will (or should) be achieved as a result of the proposed Contract Change.  | Choose an item. |
| 5   | Where the Service Provider proposes an increase in Charges, the increase must be justified by including an analysis of the reasons why costs will be impacted by the change. Supporting documentation is to be provided. | Choose an item. |
| 6   | Ensure that any increase in the Charges is consistent with the charging principles for the Services.   | Choose an item. |

Signature: [Redacted]  
 Email: [Redacted]@london-fire.gov.uk

Signature: [Redacted]  
 Email: [Redacted]@bt.com

E-signed 2023-06-28 01:34PM GMT+1  
 [Redacted]@london-fire.gov.uk



E-signed 2023-06-28 01:50PM GMT+1  
 [Redacted]@bt.com

BT



**Invitation to Provide  
a Proposal for  
Supply of a Cyber-  
Threat Detection  
and Defence System**

Date: March 2023  
Ref: PROC/7108/23

## LONDON FIRE COMMISSIONER

### Contents

|  |                              |
|--|------------------------------|
| <b>SECTION A: INSTRUCTIONS AND TENDER REQUIREMENTS</b> ..... | <b>3</b>                     |
| 1. Key Information for Tenderers .....                       | 3                            |
| 2. Conditions for Tendering.....                             | 3                            |
| 3. Submission of Tenders.....                                | 4                            |
| 4. Evaluation Process .....                                  | Error! Bookmark not defined. |
| 5. Specification .....                                       | 6                            |
| 6. Responsible Procurement Guidance.....                     | 6                            |
| <b>SECTION B: TENDER RESPONSE REQUIREMENTS</b> .....         | <b>7</b>                     |
| 1. Method Statement .....                                    | 7                            |
| 2. Mandatory Information Required .....                      | 7                            |
| 3. Form of Tender .....                                      | 8                            |
| 4. Pricing Model (if required).....                          | Error! Bookmark not defined. |

## SECTION A: INSTRUCTIONS AND TENDER REQUIREMENTS

### 1. Key Information for Tenderers

- 1.1. The London Fire Commissioner ('The Commissioner') is seeking a proposal ("the Tender") for the Supply of a Cyber-Threat Detection and Defence System under the Pan-London ICT Framework, in accordance with the attached documents.
- 1.2. The Agreement will be for a Term of three years commencing in July 2023 with the option to extend by two further years.
- 1.3. The Tenderer is required to submit a Tender proposal, with all information requested in Part B of this document, by the Tender Response deadline stated below.
- 1.4. Tenders must be open for acceptance for a period of six months following the deadline for submission of tenders.
- 1.5. Below is a timetable of the contract award process that the Commissioner will be following.

| ACTIVITY  | Date                                   |
|---|--|
| Publication of the Invitation to Provide a Proposal   | Wednesday 1 <sup>st</sup> March 2023   |
| Deadline for submission of a Tender to the Commissioner Contract ("Tender Submission Deadline") | 5pm Friday 24 <sup>th</sup> March 2023 |
| Contract Award Date   | By end of June 2023                    |
| Expected commencement date for the Contract   | July 2023                              |

- 1.6. The Commissioner reserves the right to alter this timetable.

### 2. Conditions for Tendering

- 2.1. Persons proposing to submit a Tender are advised first to read the Invitation to Tender carefully to ensure that they are fully familiar with the nature and extent of the obligations to be accepted by them if their Tender is accepted. No claims by the Contractor for additional payments will be allowed on the grounds of misunderstanding or misinterpretation due to lack of knowledge of the requirements set out in the Invitation to Tender.
- 2.2. No alterations may be made to any response document required to be submitted with your tender response. Any alteration made may result in your tender being rejected.
- 2.3. The Tender must not be:
  - 2.3.1. qualified; or
  - 2.3.2. conditional; or
  - 2.3.3. accompanied by statements which could be construed as rendering it equivocal and/or submitted on a different footing from those of other Tenderers.

- 2.4. The Commissioner is not bound to accept the lowest or any Tender and shall not be responsible for any costs in connection with the preparation thereof. If and when a Tender is accepted a written notification will be sent to each Tenderer.
- 2.5. Tender prices shall be fixed and inclusive of everything required to supply the Goods and Services but exclusive of Value Added Tax.
- 2.6. The Commissioner may decide not to award a contract to the tenderer submitting the most economically advantageous tender where it has established that the Tender does not comply with applicable obligations in the fields of environmental, social and labour law established by EU law, national law, collective agreements or by the international environmental, social and labour law provisions listed in the Public Contracts Directive (2014/24/EU) as amended from time to time.
- 2.7. Should a Tenderer be in doubt as to the interpretation of any part of the Invitation to Tender they should submit their enquiry by email.

### **3. Submission of Tenders**

- 3.1. All documents, discussions and meetings will be conducted in English. Tenders and supporting documents must be priced in Pound Sterling (£) and all payments under the contract will be made in Pound Sterling. Price variances will be considered only at the contract review opportunities expressly stated in the contract.
- 3.2. Tenderers should submit their Tender document and all required supporting documentation via email by no later than the Tender Submission Deadline. Please note that incomplete or late submissions may be rejected prior to evaluation.
- 3.3. Tenderers must return completed documentation from all requirements in Section B of the Invitation to Tender. Failure to comply fully may render your tender invalid.
- 3.4. Tenderers shall submit their solution in the form set out in Section B with their Tender as a separate document.
- 3.5. As the response of the successful Tenderer will be incorporated into the Agreement between the parties, it is vital that method statements, proposed solutions or claims are realistic and thorough but do not contain promises of a level of service which cannot be provided, achieved or maintained.
- 3.6. The successful Tenderer may be required to provide a parent company guarantee prior to the Commissioner entering into a contract. This will be largely in the form shown in the contract.
- 3.7. To reduce the impact on the environment, Tenderers are requested not to submit any promotional or marketing material with their Tender.

### **4. Tender Evaluation**

- 4.1. The Commissioner will evaluate the Tenders in accordance with the award criteria detailed in this ITT and as part of the evaluation process will select from the valid and compliant Tenders received, the Contractor that achieves the highest score against the award criteria.
- 4.2. The Commissioner will assess responses in accordance with the following award criteria:



**Technical criteria (weighted at 60%)**

- All of the technical criteria assessment will be based on responses to Section B.
- Weightings are provided for each section and for each sub-section

**Commercial criteria (weighted at 30%)**

- Full cost for the hardware, software, license and support to meet this tender requirement.
- Installation and configuration services (incl. training services)

**Responsible Procurement Guidance (weighted at 10%)**

- Response to Section 6

4.3. Scores for the Tender against the award criteria will be evaluated on the basis of '1' to '5' as set out in the table below:

| Score | Percentage | Classification | Evaluation Description   |
|-------|------------|----------------|--|
| 0     | 0%         | None           | No response, or a response which does not address the criteria.  |
| 1     | 20%        | Very Poor      | The response is of a very poor standard, which partially addresses, but has significant omissions leaving the Commissioner with a significant lack of confidence that the solution will meet the Commissioner 's requirements. |
| 2     | 40%        | Poor           | The response is of a poor standard, which partially addresses the criteria and leaves the Commissioner lacking confidence that the solution will meet the Commissioner 's requirements.  |
| 3     | 60%        | Average        | The response is of a good standard, fully addressing the required criteria and leaving the Commissioner with confidence that the solution will meet the Commissioner 's requirements..   |
| 4     | 80%        | Good           | The response is of a high standard, fully addressing the required criteria and leaving the Commissioner with a high level of confidence that the solution will meet the Commissioner 's requirement.                           |
| 5     | 100%       | Excellent      | The response is of a very high standard, fully addressing the required criteria leaving the Commissioner with a very high level of confidence that the solution will meet the Commissioner 's requirements.                    |

- 4.4. The Commissioner will evaluate the qualitative Tender responses in accordance with the above scoring matrix. The score will then be applied to the section weighting to give a weighted score for each qualitative criteria.
- 4.5. Where 'no evidence' is given, such that a zero score is recorded, then grounds will exist for excluding that Tender from further consideration. For any Tenders so excluded, the relevant price score will also be excluded from the evaluation.
- 4.6. Price will be evaluated on the basis of awarding the full percentage points available for each criterion to the lowest priced bid. A percentage score proportionate to the lowest price will be awarded to the other tendered prices using the following calculation:

$$\frac{\text{Lowest Tender price}}{\text{Tender price}} \times \text{price criteria weighting} = \% \text{ Score}$$

- 4.7. Combining both the score for the qualitative and pricing elements, the Commissioner will select the most economically advantageous Tender with the highest score against the Tender evaluation criteria.
- 4.8. The Commissioner is not bound to accept the lowest or any Tender which is non compliant with the Statement of Requirements. If and when a Tender is accepted a written notification will be sent to each Tenderer.

## 5. Specification

- 5.1. Full details of the requirements for the supply of a cyber-threat detection and defence system are set out at Annex A.

## 6. Responsible Procurement Guidance

- 6.1. The Commission is a signatory to the [GLA Group Responsible Procurement Policy](#) and expects Contract Managers and Suppliers to work towards improvements across all relevant themes throughout the delivery of goods and services.
- 6.2. Suppliers are required to provide details of any relevant product certification OR where use of these certification standards is considered unsuitable, or Suppliers are unable to offer certified products, Suppliers must:
  - i. Disclose the proposed sites of production for the contract and all Sub Contractors ;  
and
  - ii. Provide evidence to demonstrate they and their subcontractors meet the ETI Base Code.
- 6.3. Suppliers are required to disclose details of any zero hours contracts to be used in the delivery of the Services.
- 6.4. Tenderers are required to provide a valid copy of international standard certification such as ISO14001/ISO50001/ISO14040/ISO55000 , where relevant.

## **SECTION B: TENDER RESPONSE REQUIREMENTS**

### **1. Method Statement**

- 1.1. Tenderers are required to submit a method statement with their Tender which will be used in the tender evaluation process.
- 1.2. The method statement provides Tenderers with the opportunity to demonstrate their proposals for delivering quality services assessed against the evaluation criteria.
- 1.3. As the method statement of the successful Tenderer will be incorporated into the Agreement between the parties, it is vital that the method statement is realistic and thorough but does not contain promises as to the level of service which cannot be provided, achieved or maintained.
- 1.4. In preparing the method statement, the tenderer is to address the following headings and in the sequence as follows:

| <b>Ref</b> | <b>Method Statement Questions</b>  | <b>Overall Weight</b> |
|------------|--|-----------------------|
| 1          | Please detail your full solution methodology demonstrating how you meet all of the Commissioner's requirements set out in the specification and also provide full responses to the questions set out below | 60%                   |
| 2          | Please provide a firm overall price for the initial 3 year contract (with a full breakdown of pricing for each year) and confirm the firm price of the two year extension option                           | 30%                   |
| 3          | Provide a full response to the Responsible Procurement Guidance  | 10%                   |

### **Mandatory Information Required**

#### **Tenders are required to:**

- 1.5. Submit a copy of their anti-bribery policy in their Tender.
- 1.6. Supply evidence with their Tender of the anti-collusion policies and practices that the Tenderer has implemented.
- 1.7. Confirm with a YES/NO answer in their tender and provide details of the use of any Zero Hour Contracts within their organisation and that of any of their sub-contractors involved in directly delivering the contract to the Commissioner .
- 1.8. Submit a copy of their Equality Policy in their Tender and details of any equality standards they have met.
- 1.9. Submit a valid certificate for an environmental quality standard based on the principles of EN ISO 14001 (or equivalent).
- 1.10. Provide a continuity plan for the continuing provision of the supplies/services in the event of a demand, including an increased demand, for supplies/services in the event of an emergency in their Tender.
- 1.11. Provide information detailing which elements of the work are to be subcontracted.

## **Environment**

- 1.12. Outline how they will reduce the impact of their carbon emissions on the environment. This should include as a minimum identifying monitoring and reporting processes in place; priority areas for reducing emissions related to the contract, and planned actions and timeframes to address those priority areas.

---

## **Ethical Sourcing Guidelines**

- 1.13. Provide a Slavery and Human Trafficking statement, if the Tenderer has a turnover in excess of £36 million.
- 1.14. Demonstrate how they comply with the basic standards of the ETI Base Code.
- 1.15. Provide details of the main supply chain partners used for the production of the Goods to be provided, including the location and registered number of the manufacturing site(s).
- 1.16. For manufacturing sites not registered under any quality assurance scheme, identify the quality assurance procedures that are maintained or show evidence of progress towards achieving registration to a scheme.

## **Key Contracts**

- 1.17. Provide relevant third-party certifications addressing ethical issues within the Tenderers supply chain or equivalent third-party certifications. Certification must be specific to the product or site of production and a requirement to maintain up-to-date certification must be included in the contract.
- 1.18. Verify compliance with the Base Code of the Ethical Trade Initiative (ETI) (see Appendix 3), suppliers should provide a relevant third-party certification which covers the specific products or manufacturing sites proposed for the contract. Tenderers are required to complete the Sedex Self-Assessment Questionnaire (SAQ) and submit this with their Tender. Alternatively, the tenderer is required to:
  - Disclose the proposed sites of production for the contract and all subcontractors,
  - Provide evidence to demonstrate they and their subcontractors meet the ETI Base Code.
- 1.19. Provide a Statement on Slavery and Human Trafficking in their supply chain with their tender, if the tenderer has a turnover in excess of £36 million, to whom the requirements of Part 6 of the Modern Slavery Act 2015 apply.

## **Waste**

- 1.20. Identify any take back schemes the Tenderer operates or that are operated on their behalf related to this contract, if the Tenderer is not part of the Distributor Take back Scheme.
- 1.21. Give any other aspect which the Tenderer considers to be generally necessary.

## **2. Form of Tender**

**To: The London Fire Commissioner**

I/We the undersigned hereby offer to provide the Services set out in the Invitation to Tender for the Charges set out at in the Tender.

**By signing this Form of Tender you are providing confirmation that the Tender has been fully completed**

**No. of hours in a Business Day** \_\_\_\_\_

And I/we agree that this Tender shall remain open for acceptance for six calendar months from the specified date for receipt of this Tender. I/We undertake that I/we have not communicated and will not communicate to any person other than the Commissioner the amount of this Tender and that I/we have not adjusted the amount of the Tender in accordance with any arrangement between me/us and any other firm or company. I/We undertake that I/we have not:

1. Entered into any arrangement with any other person with the aim of preventing a tender or fixing or adjusting the amount of this Tender or the conditions on which the Tender is made; or
2. Communicated to any person other than the Commissioner the amount of this Tender except where the disclosure, in confidence, of the amount was necessary to obtain quotations for the preparation of this Tender for insurance, performance bonds and/or contract guarantee bonds or for professional advice required for the preparation of the Tender; or
3. Caused or induced any person to enter into such an arrangement set out in paragraphs 1. and 2. above; or
4. Communicated to the Commissioner the amount or the approximate amount of any rival tender for the Services; or
5. Committed any offence under the Prevention of Corruption Acts 1889 to 1916 nor under Section 117 of the Local Government Act, 1972; or
6. Offered or agreed to pay or give any sum of money, inducement or valuable consideration directly or indirectly to any person for doing or having done or causing or having caused to be done in relation to any other Tender or proposed tender for the Services any act or omission; or
7. Canvassed any other persons referred to in 1. above in connection with this Invitation to Tender; or
8. Contacted any officer of the Commissioner about any aspect of this Invitation to Tender including (but without limitation) for the purposes of discussing the possible transfer to the employment of the Tenderer of such officer for the purposes of any resulting Agreement or for soliciting information in connection with the Services.

I/We also undertake that I/we will not procure the doing of any acts set out in paragraphs 1. to 8. above before the specified hour and date for receipt of this Tender nor (in the event of this Tender being accepted) shall I/we do so while the resulting Agreement continues in force between us.

In this Form of Tender the word "person" includes any person, body or association, corporate or incorporate and "arrangement" includes any arrangement whether formal or informal and whether legally binding or not.

Dated \_\_\_\_\_  
Full name of firm or company  
(including trading name if  
applicable) \_\_\_\_\_  
Company Registration Number \_\_\_\_\_  
VAT No \_\_\_\_\_  
Signature (original required)  
(in the case of a firm or company,  
duly authorised to sign in that  
behalf) \_\_\_\_\_  
Name in block capitals \_\_\_\_\_  
Designation \_\_\_\_\_  
Address \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
Post code \_\_\_\_\_  
Telephone number \_\_\_\_\_  
Fax No \_\_\_\_\_  
Email address \_\_\_\_\_

## **Appendix 1 - The Ethical Trading Initiative Base Code**

### **Part 1**

Please note that section 1.2 and 1.6.2 have been removed, and 1.6.1 has been slightly altered.

#### **1.1. EMPLOYMENT IS FREELY CHOSEN**

- 1.1.1. There is no forced, bonded or involuntary prison labour.
- 1.1.2. Workers are not required to lodge "deposits" or their identity papers with their employer and are free to leave their employer after reasonable notice.

#### **1.2. NOT USED**

#### **1.3. WORKING CONDITIONS ARE SAFE AND HYGIENIC**

- 1.3.1. A safe and hygienic working environment shall be provided, bearing in mind the prevailing knowledge of the industry and of any specific hazards. Adequate steps shall be taken to prevent accidents and injury to health arising out of, associated with, or occurring in the course of work, by minimising, so far as is reasonably practicable, the causes of hazards inherent in the working environment.
- 1.3.2. Workers shall receive regular and recorded health and safety training, and such training shall be repeated for new or reassigned workers.
- 1.3.3. Access to clean toilet facilities and to potable water, and, if appropriate, sanitary facilities for food storage shall be provided.
- 1.3.4. Accommodation, where provided, shall be clean, safe, and meet the basic needs of the workers.
- 1.3.5. The company observing the code shall assign responsibility for health and safety to a senior management representative.

#### **1.4. CHILD LABOUR SHALL NOT BE USED**

- 1.4.1. There shall be no new recruitment of child labour.
- 1.4.2. Companies shall develop or participate in and contribute to policies and programmes which provide for the transition of any child found to be performing child labour to enable her or him to attend and remain in quality education until no longer a child.
- 1.4.3. Children and young persons under 18 shall not be employed at night or in hazardous conditions.
- 1.4.4. These policies and procedures shall conform to the provisions of the relevant ILO standards.

#### **1.5. LIVING WAGES ARE PAID**

- 1.5.1. Wages and benefits paid for a standard working week meet, at a minimum, national legal standards or industry benchmark standards, whichever is higher. In any event wages should always be enough to meet basic needs and to provide some discretionary income.
- 1.5.2. All workers shall be provided with written and understandable Information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid.

1.5.3. Deductions from wages as a disciplinary measure shall not be permitted nor shall any deductions from wages not provided for by national law be permitted without the expressed permission of the worker concerned. All disciplinary measures should be recorded.

**1.6. WORKING HOURS ARE NOT EXCESSIVE**

1.6.1. Working hours comply with at least UK national laws and benchmark industry standards, whichever affords greater protection.

1.6.2. Not used.

**1.7. NO DISCRIMINATION IS PRACTISED**

1.7.1. There is no discrimination in hiring, compensation, access to training, promotion, termination or retirement based on race, caste, national origin, religion, age, disability, gender, marital status, sexual orientation, union membership or political affiliation.

**1.8. REGULAR EMPLOYMENT IS PROVIDED**

1.8.1. To every extent possible work performed must be on the basis of recognised employment relationship established through national law and practice.

1.8.2. Obligations to employees under labour or social security laws and regulations arising from the regular employment relationship shall not be avoided through the use of labour-only contracting, sub-contracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment, nor shall any such obligations be avoided through the excessive use of fixed-term contracts of employment.

**1.9. NO HARSH OR INHUMANE TREATMENT IS ALLOWED**

1.9.1. Physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation shall be prohibited.

**Note on the Provisions of this Code**

The provisions of this code constitute minimum and not maximum standards, and this code should not be used to prevent companies from exceeding these standards. Companies applying this code are expected to comply with national and other applicable law and, where the provisions of law and this Base Code address the same subject, to apply that provision which affords the greater protection.

**Part 2 – Definitions**

2.1. **Child** : Any person less than 15 years of age unless local minimum age law stipulates a higher age for work or mandatory schooling, in which case the higher age shall apply. If however, local minimum age law is set at 14 years of age in accordance with developing country exceptions under ILO Convention No. 11, the lower will apply.

2.2. **Young person**: Any worker over the age of a child as defined above and under the age of 18.

2.3. **Child labour**: Any work by a child or young person younger than the age(s) specified in the above definitions, which does not comply with the provisions of the relevant ILO standards, and any work that is likely to be hazardous or to interfere with the child's or young person's education, or to be harmful to the child's or young person's health or physical, mental, spiritual, moral or social development



### 3. Appendix 2 -Blacklisting Policy

1. The Employment Relations Act 1999 (Blacklists) Regulations 2010\* states that no person shall compile, use, sell or supply a prohibited list which a) contains details of persons who are or have been members of the trade unions or persons who are taking part or have taken part in the activities of trade unions, and b) is compiled with a view to being used by employers or employment agencies for the purposes of discrimination in relation to recruitment or in relation to the treatment of workers.
2. The Commissioner imposes strict obligations upon all bidders and contractors in terms of compliance with statutory provisions, including blacklisting such as required by the Employment Relations Act 1999 (Blacklists) Regulation 2010 in line with the provisions of the Employment Relations Act 1999 (Blacklists) Regulations 2010, The Commissioner is of the view that 'blacklisting' may constitute grounds for discretionary exclusion under Regulation 57(8)© of the Public Contracts Regulations 2015.
3. The Commissioner respects the rule of law in all our commitments and has a minimum standard compliance with all law and regulation to which our businesses are subject. The Commissioner does not condone or tolerate Blacklisting.
4. The procurement process shall include questions and obligations upon bidders to these effects. Non compliance may result, where applicable, in a bidder being deselected from a procurement process, or may result in a contract not being awarded, or may result in a contract being terminated. If your company is found to engage in blacklisting after the awarding of a contract, or it comes to light that the company engaged in blacklisting in the past but has failed to declare this in the tendering process, The Commissioner will act to terminate the contract. Failure to comply will put The Commissioner at risk and may result in potentially significant legal, financial, reputational and personal consequences.
5. The Commissioner will consider business with a bidder or contractor who can demonstrate that it has taken appropriate remedial steps, and has self cleansed.
6. Remedial steps may include the following actions:
  - 6.1. The provision of an appropriate apology acknowledging wrong-doing in relation to the compiling, use, selling or supplying of blacklists with the view of discriminating against workers and/or the discrimination against an individual in terms of their trade union membership status;
  - 6.2. The provision of a statement regarding future conduct;
  - 6.3. The collaboration with investigating authorities to clarify the facts and circumstances in a comprehensive manner;
  - 6.4. The implementation of concrete, technical, organisational and personnel measures that are appropriate to prevent further criminal offence or misconduct;
  - 6.5. Full compliance with any tribunal ruling; and
  - 6.6. The payment of compensation in respect of any damage caused by any wrong-doing.
7. The bidder or contractor will be obliged to ensure they are fully compliant and aware of the Blacklisting Policy. The Commissioner will not be responsible for making a decision or assessing the respective bidder / contractor with regards to its Blacklisting status. The Commissioner expects all engagements to be compliant in line with the statutory provisions.

**Solution – Additional Questions**

In this section a response is required to all questions. Compliance with evaluation criteria and weighting detailed in section 11 will be determined from tenderers responses to these questions.

A number of mandatory requirements are detailed in APPENDIX 1. Tenderers must clearly indicate if they meet each of the requirements. If a tenderer does not meet all of the mandatory requirements, then they shall be disqualified from consideration.

A number of qualitative questions are detailed in APPENDIX 2. Tenderers must respond to all questions. A weighting has been applied to each question. Responses to each question will be scored according to the table below.

**APPENDIX 1 – Mandatory requirements**

Tenderers must respond to all Questions

*Failure to answer any of the sections below will invalidate your tender response and will cause it to be excluded from the competition.*

| Ref | Requirement description  | Does your proposal meet requirement (Yes or No)? | Please use this section to describe either how your solution meets the requirement or to provide more detail. Please include references to technical articles/reviews/specifications |
|-----|--|--|--|
| M1  | The solution must be capable of learning a pattern of life for every network, device and user, correlating this information to spot subtle deviations and lateral movement that indicate in-progress threats |  |  |
| M2  | The solution must be capable to detect malware, APTs, insider threats as well as previously unknown attacks, or 'unknown unknown', zero-day attacks  |  |  |
| M3  | The solution must be able to intelligently auto-classify and prioritise threats while still supporting workflow and collaboration  |  |  |
| M4  | The solution must provide 100% network visibility in real time, including visibility into SaaS, Cloud, and virtualized environments  |  |  |
|     |  |  |  |
|     |  |  |  |

## APPENDIX 2 – Evaluation Questions

Tenderers must respond to all Questions

*Failure to answer any of the sections below will invalidate your tender response and will cause it to be excluded from the competition.*

| Ref | Sub-Weighting of 70% |   |
|-----|----------------------|---|
| A1  | 20                   | Describe how the proposed solution is capable of unsupervised machine learning of standard network activity and adaptive to normal organizational business, and capable of recognising anomalous network activity.<br>If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information. |
| A2  | 10                   | Describe how the proposed solution is capable of base lining a network environment in real time without prior knowledge of the environment. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.   |
| A3  | 10                   | Describe how the proposed solution learns a pattern of life for every network, device and user, correlating this information to spot subtle deviations and lateral movement that indicate in-progress threats<br>If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.      |
| A4  | 10                   | Describe how the proposed solution is able to detect malware, APTs, insider threats as well as previously unknown attacks, or 'unknown unknown', zero-day attacks and VXLAN encapsulation. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.                            |
| A5  | 10                   | Describe how the proposed solution intelligently auto-classifies and prioritises threats while still supporting workflow and collaboration. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.   |
| A6  | 10                   | Demonstrate how the proposed solution provides 100% network visibility in real time, including visibility into SaaS, Cloud, and virtualized Environments. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.   |
| A7  | 10                   | Describe how the proposed solution provides a register of all assets detected on the network. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.   |
| A8  | 10                   | Describe how the proposed solution is self-configuring; works automatically and does not require tuning or configuration to suit the specific network. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.  |
| A9  | 5                    | Please provide details of your proposed support model (Minimum Requirements: 9-5 Helpdesk incl health checks, analyst support and hardware fixes). If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.  |
| A10 | 5                    | Alerting must be able to be outputted to email, SMS, SIEM and other security tools. If you feel you have answered this question previously, please refer to that answer in your response and do not re-type the same information.   |

## Cyber Defence Specification

### **Purpose**

The London Fire Brigade ("LFB") are looking to engage a supplier to supply a cyber-threat detection and defence system.

### **Requirements**

#### Core Solution Requirements

The tender invites a single comprehensive response to this requirement. LFB wish to procure an unsupervised cyber threat detection and defence system which will be deployed at the LFBs network down to device and user level to monitor and detect abnormal network behaviour as well as threats such as malware and advanced persistence threat (APT). The solution should be capable of operating in respect of both on premise and cloud based infrastructure, including MS 365.

Tenderers should note the desired functionality detailed below in respect of any solution proposed:

- The solution must be capable of unsupervised machine learning of standard network activity and adaptive to normal organisational business, and capable of recognising anomalous network activity.
- The solution must have the capability of base lining a network environment in real time without prior knowledge of the environment and support update to the new normal.
- The solution must be capable of learning the pattern of life for every network, device, and user, correlating this information to spot subtle deviations and lateral movement that indicate in progress threats.
- The solution must be able to detect previously unknown attacks, or 'unknown unknown', zero day attacks.
- The solution must be able to detect not only malware, but also APTs and insider threat
- The solution should not solely rely on rules or signatures, but rather Bayesian statistical models, behavioural analysis and unsupervised machine learning to more accurately detect real world threats
- The solution should be able to intelligently auto-classify and prioritise threats, supporting workflow and collaboration
- The solution must provide 100% network visibility in real time, including visibility into SaaS, Cloud, and virtualized environments: VxLAN encapsulation, desirable double VxLAN encapsulation capability.
- The solution should be able to model and spot threats emerging from IOT devices
- The solution must be able to spot attacks at any point in their life cycle
- The solution should be able to graphically display network events and have a user interface that is not only suitable for analysts but information security teams
- The solution must be able to provide a register of all assets detected on the network
- The solution should be able to accurately detect true anomalies for any environment it is deployed onto
- The solution should be intelligent enough to automatically filter out false positives
- The solution should be customisable to allow clients to build their own models to suit their individual business needs and focus on their specific areas of concern
- The solution should also be able to self-configure and work automatically on any network

- The solution should be passive TAP, SPAN, or Netflow.
- Alerting must be able to be outputted to email, SMS, SIEM and other security tools

#### **Users/Devices**

Approx. Number of Users: 6000

Approx. Number of Devices: 2400 laptops, up to 50 physical servers / 400 virtual servers / 180 virtual terminal servers.

#### **Implementation and Configuration Services**

Tenderers should identify hardware installation and software configuration services as part of their proposed solution as well as on-site training on the proposed solution. If these services incur additional costs please include this in the pricing schedule below, these costs will be factored into the pricing element of the evaluation (LFB will not be liable for any expenses incurred from the delivery of these additional services). Please note that we intend to procure an "opex" or "revenue" based system and so all costs should be split over the term of the contact.

#### **Services should include:**

- Installation and Client configuration
- Quality Assurance of customer implementation
- Supporting documentation and handover
- On-site system familiarisation for up to 6 people (min. 2 Days Training) including training manuals (this training will only be scheduled after the proof of concept/trial period is complete and formal award of the contract). However, some initial training to be provided so that staff can use the system and asses how it functions as part of the pilot / testing stage.

#### **Support & Maintenance and Software Subscriptions**

Support should be available with the minimum level requirements of; Access to a helpdesk operating 24/7, Proactive Threat Notification 24/7, Customer Portal, health checks, analyst support and software/hardware support and fixes.

For the proposed solution all support and maintenance subscriptions required should be based on the initial 36 month term with fixed pricing for the optional 2 x 12 month extension periods and be fully inclusive of all updates. These costs should be clearly stated within the pricing schedule.