GREATER**LONDON**AUTHORITY

REQUEST FOR DEPUTY MAYOR FOR FIRE DECISION – DMFD241

Procurement of managed security information and event management service

Executive summary:

This report requests the approval of the Deputy Mayor for the Fire Service (Deputy Mayor) to authorise the London Fire Commissioner (LFC) to commit revenue expenditure of up to the amount stated in part two of this report for the procurement of a managed security information and event management (SIEM) service. A SIEM system helps organisations detect, analyse, and respond to security threats before they have the opportunity to harm business operations. The system collects "event" log data from a range of sources and analyses a high volume of data in seconds to alert on activity that deviates from the norm with real-time analysis. The LFC proposes to enter into a contact with an external organisation to manage the SIEM on behalf of the LFC. This will ensure that security alerts are appropriately acted on and prioritised by dedicated analysts, to provide crucial insight and expertise 24 hours per day, seven days per week.

The London Fire Commissioner Governance Direction 2018 sets out a requirement for the LFC to seek the prior approval of the Deputy Mayor before "[a] commitment to expenditure (capital or revenue) of £150,000 or above as identified in accordance with normal accounting practices".

Decision:

That the Deputy Mayor for the Fire Service authorises the London Fire Commissioner to commit expenditure up to the amount set out in Part Two of the report, for the procurement of a managed security information and event management service.

Deputy Mayor for Fire and Resilience

I confirm that I do not have any disclosable pecuniary interests in the proposed decision.

The above request has my approval.

Signature:

Date:

29/08/2024

PART I – NON-CONFIDENTIAL FACTS AND ADVICE TO THE DEPUTY MAYOR

Decision required – supporting report

1. Introduction and background

1.1 Report LFC-24-049x to the London Fire Commissioner (LFC) explains that the security threat posed to organisations around the globe from cyber-attacks (including ransomware/malware, data extortion and associated threats) has increased exponentially in recent years. The ongoing situation in Ukraine has resulted in an increased threat level to the UK, as a result of hostile cyber events emanating from a range of sources, including state actors.

1.2 The LFC regularly receives security information from a range of sources, including central and local government, other fire and rescue services (FRSs), and specialist security organisations. The government's current is that, whilst there is no specific threat emanating from hostile actors in relation to London Fire Brigade (LFB), there is a risk of organisations suffering collateral damage in the event of a sophisticated cyber-attack against the UK.

1.3 The threat from cyber criminals continues to grow, with capability predicted to increase over the next two years due to advancements in artificial intelligence (AI)[1] and exploitation of this technology. In recognition of the ever-increasing threat posed to LFC systems and data by the cyber threat, the LFC has installed a cyber-defence system, Darktrace. This uses AI and machine learning to initially define a "normal" state; and then detect anomalies, and take autonomous action to neutralise threats.

1.4 However, in recognition of the current risk landscape, it is now considered essential for organisations to have multi-layered defences, offering "strength in depth", when it comes to the security of information and assets. Whilst Darktrace may be considered the ultimate line of defence to cyber threats, a security information and event management (SIEM) system is concerned with rapidly consuming and analysing large volumes of information from a wide range of sources; identifying anomalies; and alerting on suspicious behaviour, before an actual security incident occurs.

2. Objectives and expected outcomes

2.1 The LFC currently uses Sentinel, a Microsoft SIEM system that has been configured to interface with a small number of LFC systems. However, it is clear that once the SIEM system is fully deployed, the amount of information provided will be significant, and consume scarce security-team resource. It is therefore considered that the security needs of the LFC could better be met by contracting with an external organisation to provide the SIEM as a service.

2.2 Therefore, the LFC wishes to enter into a contract, in 2024-25, with an external organisation to manage the SIEM on behalf of the LFC. This provides an opportunity to ensure that security alerts are appropriately acted on and prioritised by dedicated analysts, and to provide crucial insight and expertise 24 hours a day. In addition, the solution by design will be scalable. This means that, as the number and complexity of LFC systems increases, and services continue to be migrated from on-premises to the cloud,[2] the managed service can "flex" to accommodate this with fast deployment and reduced setup costs.

3. Equality comments

[1] AI is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities

[2] "The cloud" is the name given to a global network of remote servers that operates as a single ecosystem, commonly associated with the internet.

3.1 The LFC and the Deputy Mayor for the Fire Service (the Deputy Mayor) are required to have due regard to the Public Sector Equality Duty (section 149 of the Equality Act 2010) when taking decisions. This in broad terms involves understanding the potential impact of policy and decisions on different people; taking this into account; and then evidencing how decisions were reached.

3.2 It is important to note that consideration of the Public Sector Equality Duty is not a one-off task. The duty must be fulfilled before taking a decision, at the time of taking a decision, and after the decision has been taken.

3.3 The protected characteristics are: age, disability, gender reassignment, pregnancy and maternity, marriage and civil partnership (but only in respect of the requirements to have due regard to the need to eliminate discrimination), race (ethnic or national origins, colour or nationality), religion or belief (including lack of belief), sex, and sexual orientation.

3.4 The Public Sector Equality Duty requires decision-takers in the exercise of all their functions, to have due regard to the need to:

- eliminate discrimination, harassment and victimisation and other prohibited conduct
- advance equality of opportunity between people who share a relevant protected characteristic and persons who do not share it
- foster good relations between people who share a relevant protected characteristic and persons who do not share it.

3.5 Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:

- remove or minimise disadvantages suffered by persons who share a relevant protected characteristic where those disadvantages are connected to that characteristic
- take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it
- encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.

3.6 The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

3.7 Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:

- tackle prejudice
- promote understanding.

3.8 An equalities impact assessment has not been carried out for this procurement. The introduction of a managed SIEM service should be entirely transparent to LFC staff.

4. Other considerations

Workforce comments

4.1 There are no plans for workforce consultation.

Sustainability comments

4.2 This report discusses a managed SIEM service that will help LFB detect, analyse and respond to security threats before they have the opportunity to harm business operations.

4.3 This report does not introduce any significant sustainability impacts. Where new policies and/or corporate projects arise, they are subject to LFB's sustainable development impact assessment process.

Procurement comments

4.4 LFB's Procurement department will identify a suitable route to market once the procurement starts. The GLA Collaborative Procurement Board has been formally approached regarding collaboration in respect of this procurement. However, the LFC has been advised that there are currently no collaborative opportunities available in respect of a managed SIEM service.

4.5 The National Fire Chiefs Council (NFCC) has been approached with the intention of identifying collaboration opportunities. The NFCC has no specific plans to develop a managed SIEM system for the sector. However, plans are being developed to establish a "security operations centre" for the FRS sector. The prerequisite for joining this service will be that each FRS has implemented its own SIEM system (or service). It is anticipated to be at least three years until the LFC can join in this sector initiative, which will provide a range of services in the security space.

4.6 If appropriate, procurement will assess the market and/or conduct some early market engagement with suppliers to ensure there is an appetite for the requirements; and to test routes to market, such as the Crown Commercial Service framework, Cyber Security Services 3.

4.7 The proposed new contract is intended to be for five years; the funding requested in Part 2 supports this. The procurement team will work with the Information and Communications Technology (ICT) department to agree an optimum contract duration. For example, this could be an initial three-year contract, with the ability to extend the contract by up to two years; but this will be confirmed before issuing the opportunity to market.

Conflicts of interest

4.8 There are no conflicts of interest to declare from those involved in the drafting or clearance of this decision.

5. Financial comments

5.1 The report seeks authority for the LFC to enter into a contract to provide a managed SIEM service.

5.2 The estimated cost of the service is set out in Part Two of this report.

5.3 There are no direct financial implications for the GLA.

6. Legal comments

6.1 Under section 9 of the Policing and Crime Act 2017, the LFC is established as a corporation sole with the Mayor appointing the occupant of that office. Under section 327D of the GLA Act 1999, as amended by the Policing and Crime Act 2017, the Mayor may issue to the LFC specific or general directions as to the manner in which the holder of that office is to exercise his or her functions.

6.2 By direction dated 1 April 2018, the Mayor set out those matters, for which the LFC would require the prior approval of either the Mayor or the Deputy Mayor.

6.3 Paragraph (b) of Part 2 of that direction requires the LFC to seek the prior approval of the Deputy Mayor before "[a] commitment to expenditure (capital or revenue) of £150,000 or above as identified in accordance with normal accounting practices". The value of the SIEM service is set out in part 2 to this report and exceeds this threshold. The Deputy Mayor's approval is therefore required.

6.4 The SIEM service proposal is consistent with the LFC's power under:

- section 7 (2)(a) of the Fire and Rescue Services Act 2004, under which the LFC must secure the provision of personnel, services and equipment necessary to efficiently meet all normal requirements for firefighting
- section 5A of the Fire and Rescue Services Act 2004, under which the LFC may do anything they consider appropriate for purposes incidental to their functional purposes.

This includes the provision of ICT equipment and the necessary cybersecurity measures to ensure their continued functionality.

6.5 Any proposed procurement will be undertaken in compliance with the Public Contracts Regulations 2015 and the LFC's standing orders and policies.

6.6 These comments have been adopted from those provided by the LFC's General Counsel Department in report LFC-24-049 to the LFC.

Appendices and supporting papers:

Appendix 1 – London Fire Commissioner report LFC-24-049 – Procurement of managed security information and event management system

Public access to information

Information in this form (Part 1) is subject to the Freedom of Information Act 2000 (FOI Act) and will be made available on the GLA website within one working day of approval.

If immediate publication risks compromising the implementation of the decision (for example, to complete a procurement process), it can be deferred until a specific date. Deferral periods should be kept to the shortest length strictly necessary. **Note:** This form (Part 1) will be published either within one working day after approval or on the defer date.

Part 1 Deferral:

Is the publication of Part 1 of this approval to be deferred? NO

Part 2 Confidentiality: Only the facts or advice considered to be exempt from disclosure under the FOI Act should be in the separate Part 2 form, together with the legal rationale for non-publication.

Is there a part 2 form? YES

ORIGINATING OFFICER DECLARATION:	Drafting officer to confirm the following (✓)
Drafting officer Soeli Dayus has drafted this report with input from the LFC and in accordance with GLA procedures and confirms the following:	✓
Assistant Director/Head of Service Niran Mothada has reviewed the documentation and is satisfied for it to be referred to the Deputy Mayor for Fire and Resilience for approval.	✓
Advice The Finance and Legal teams have commented on this proposal.	✓
Mayoral Delivery Board A summary of this decision was reviewed by the Mayoral Delivery Board on 27 August 2024.	✓

INTERIM CHIEF FINANCE OFFICER:

I confirm that financial and legal implications have been appropriately considered in the preparation of this report.

Signature:

Anna Casbolt

PP Anna Casbolt on behalf of Enver Enver

Date:

29/08/2024