GREATER**LONDON**AUTHORITY

REQUEST FOR DEPUTY MAYOR FOR FIRE & RESILIENCE DECISION – DMFD28

Title: Cyber Defence System: Acceptance of Tender

Executive Summary:

Report LFC-0152 to the London Fire Commissioner seeks approval to accept a tender for the value of £212k with BT Global Services for the supply of Cyber Defence System software *DarkTrace* for the London Fire Brigade, for a period of two years. The system will protect the Brigade's information, systems and associated assets from hostile and malicious cyber threats.

The London Fire Commissioner Governance Direction 2018 sets out a requirement for the London Fire Commissioner 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:

The Deputy Mayor for Fire and Resilience:

Consents to the commitment of £212k by the London Fire Commissioner for the procurement of cyber defence services from BT Global Services.

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: 10/6/19

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

Decision required – supporting report

1. Introduction and background

1.1. In recent years, the security threat posed to organisations around the globe from cyber-attacks, malware and associated threats, has increased exponentially. The "WannaCry" ransomware attacks are a high-profile example.

1.2. On 12 May 2017, security companies noticed that a piece of malicious software known as WannaCry was spreading across the internet, first in the UK and Spain, and then around the world. It would reach 230,000 computers in 48 hours, an unprecedented scale of infection according to Europol, Europe's international police agency. WannaCry rendered useless some of the computers that help run Britain's National Health Service (NHS), causing ambulances to be diverted and shutting down non-emergency services. It also infected machines at Telefónica, Spain's biggest telecommunications company; at Hainan, a Chinese airline; and even in Russia's interior ministry.

1.3. However, whilst WannaCry was perhaps one of the more high-profile attacks, it was one of a number of attacks that have been perpetrated since the early 2000s and was not actually the worst. Other worms—Conficker, MyDoom, ILOVEYOU—caused billions of pounds of damage in the 2000s.

1.4. There is no reason to believe that the threat to systems around the world will do anything other than increase. Whilst the London Fire Brigade has multi-layered defence systems already in place such as anti-virus scanning, web-filtering and a strategy to implement security patches regularly, it currently lacks an overarching cyber defence system.

1.5. The Brigade itself was unaffected by the WannaCry ransomware. This was due in no small part to the efforts of ICT staff who worked constantly over the period in question to ensure that all reasonable precautions had been taken to protect Brigade systems against this threat. This included isolating the Brigade from the internet for a period of time.

1.6. The Brigade is looking to take positive action in relation to the ever-changing cyber threat and this will include adhering to the 'Cyber Essentials' certification (self-certification) process run by the National Cyber Security Centre (NSCC) and potentially seeking accreditation against the Cyber Essential Plus standard (which requires external accreditation).

1.7. However, as the nature and frequency of threats evolve and increase, it is clear that the Brigade needs to adopt a more proactive stance. A cyber defence system will help the Brigade to identify and minimise the chances of its operations being impacted by potential future cyber attacks.

1.8. Report LFC-0152 to the London Fire Commissioner sought approval to accept a tender for the supply of Cyber Defence System software for the Brigade. The system will protect the Brigade's information, systems and associated assets from hostile / malicious cyber threats. seeks approval to procure two now replacement Fireboats. The Commissioner's Board have considered and recommended the proposal to the Commissioner, who has indicated in-principle support pending prior consent to spend from the Deputy Mayor. The Deputy Mayor for Fire and Resilience also considered the proposals to the Commissioner in report LFC-0152 at her Fire and Resilience Board on 9 April 2019 and indicated her support.

2. Objectives and expected outcomes

Security information and event management systems (SIEM)

2.1. In determining its requirements, the Brigade initially identified a need to deploy a security information and event management system (SIEM)'. SIEM software collects and aggregates log data generated throughout the organisation's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorises incidents and events, as well as analyses them. The software delivers on two main objectives, which are to (a) provide reports on security-related incidents and events, such as successful and failed logins, malware activity and other possible malicious activities and (b) send alerts if analysis shows that an activity runs against pre-determined rulesets and thus indicates a potential security issue. Many organisations around the world have either installed such a system or are planning to do so.

2.2. Although SIEM propositions from different suppliers vary in their approach, they all share an underlying principle. That is to aggregate relevant data from multiple sources, identify deviations from an established 'norm' and to prompt appropriate action. For example, when a potential issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity's progress.

2.3. However, SIEM systems can be very resource intensive. Once data has been collected, collated and alerts/reports generated, manual intervention is regularly required to determine an appropriate course of action to be taken.

Next generation cyber defence systems

2.4. The latest generation of cyber security products use the SIEM approach but take this to the next level. Using machine learning algorithms, these products are able to operate unsupervised (to a large extent) and are able to identify, classify, prioritise and neutralise malware and advanced persistent threats (APT), using built in artificial intelligence (AI) type processes.

2.5. This means that rather than operate on logs, these next generation systems monitor raw network traffic, seeing every single device and user, and automatically learning the complex relationships between them. Having initially established a detailed understanding of what 'normal' looks like, these systems can identify emerging threats that have bypassed traditional defences and are active within a network.

2.6. Whilst these next generation cyber defence systems may be more expensive than traditional SIEM systems, the system cost really needs to be looked at in the context of the staff resources needed to respond to alerts/reports and the significant cost of a recovery from a cyber breach / ransomware attack. This is not to mention the reputational damage that might result from a cyber-attack that disables the organisation and impacts on its services.

2.7. There are numerous accounts of organisations having to spend considerable sums of money in clean-up operations from cyber-attacks / ransomware outbreaks (and that is only the ones that are reported). For example, shipping giant and NotPetya victim Maersk, was forced to replace tens of thousands of servers and computers in the aftermath of a recent ransomware attack. The cost to the business in terms of both operational and reputational loss was immense and in financial terms, far more than the anticipated cost of a defence system.

2.8. Whilst no system is able to offer a guarantee against evolving cyber threats, these new generation of cyber defence systems are better equipped to deal with 'zero-day' attacks; this is an attack that exploits a previously unknown security vulnerability. A zero-day attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

2.9. The LFB's Chief Information Officer (CIO) has discussed the threat of cyber-attack with the Senior Information Risk Officer (SIRO) on many occasions, as part of on-going meetings. The cyber-attack threat is represented on the corporate risk register and regularly reviewed. The introduction of a cyber-defence system will count as significant mitigation to this risk, although the risk can never be completely mitigated.

2.10. The introduction of a cyber defence system which does not require and minimises day to day direct supervisory effort and offers the ability to detect and prevent zero-day attacks, will ensure that the Brigade is on the front foot in the constant battle against persistent and unpredictable cyber-attacks.

2.11. On this basis, it was decided to seek to procure such a cyber defence system.

3. Equality comments

3.1. The Public Sector Equality Duty – and the potential impacts of this decision on those with protected characteristics (age, disability, gender reassignment, pregnancy and maternity, race, gender, religion or belief, sexual orientation) – has been considered by the London Fire Commissioner (and the Deputy Mayor for Fire and Resilience at the Fire and Resilience Board on 9 April 2019). The Public Sector Equality Duty applies to the London Fire Commissioner and the Deputy Mayor for Fire and Resilience when they make decisions. The Duty requires them to have regard to the need to:

a) Eliminate unlawful discrimination, harassment and victimisation and other behaviour prohibited by the Act. In summary, the Act makes discrimination etc. on the grounds of a protected characteristic unlawful.

b) Advance equality of opportunity between people who share a protected characteristic and those who do not.

c) Foster good relations between people who share a protected characteristic and those who do not including tackling prejudice and promoting understanding.

3.2. The Act states that 'marriage and civil partnership' is not a relevant protected characteristic for (b) or (c) although it is relevant for (a).

3.3. An equalities impact assessment has been carried out in respect of the implementation of this system and indicates that the system will not have a disproportionately adverse effect on any persons with a particular characteristic. The cyber defence system works in the background of the Commissioner's Information Technology environment and should be invisible to the user. It will, however, protect all users from the impacts that a cyber-attack can have on the day-to-day activities of the organisation.

3.4. The procurement of a cyber-defence system has been considered in regard to Duties (b) and (c), with no further actions required.

4. Other considerations

Procurement

4.1. The LFB Director of Corporate Services initiated the tendering process for cyber defence system software (under the delegated authority granted to her by the Commissioner) and the procurement exercise has been carried out by staff from the ICT and Procurement departments.

4.2. The procurement was carried out utilising two framework agreements:

a) Crown Commercial Service (CCS) Technology Products 2 (RM 3733, Lot 3); and

b) Pan-London ICT Framework (Lot 4).

4.3. Both frameworks were utilised in order to ensure the most economically advantageous solution was obtained for the Brigade. The advice from General Counsel was sought on this course of action before publication of the Commissioner's invitation to participate to ensure compliance with the Procurement Regulations.

4.4. An *Invitation to Participate* was published on 3 December 2018 to the 19 companies listed on the two frameworks. At the deadline for responses, four companies submitted a response, three companies notified withdrawal from the tender process, and 12 companies failed to submit a response.

4.5. The evaluation was carried out in two stages:

1) Stage one was the evaluation of the method statement and tender. The evaluation consisted of a number of mandatory pass/fail criteria. The price element was weighted at 25 percent, and the quality element at 75 per cent.

2) Stage two allowed the top three scoring tenderers from stage one to be invited to provide a presentation of their proposed solution including a live demonstration, plus a question and answer session. There was a single score for this element.

4.6. The final evaluation was a combination of the scores from stages one and two, both were given an equal weighting of 50 per cent.

4.7. During the course of the stage one evaluation, two companies were excluded from the tender process. One company failed to meet the mandatory requirements which were scored on a pass/fail basis. The other company submitted a bid which was outside the affordability envelope; it was almost four times the cost of the other two solutions based on the year-one costs alone.

4.8. The two remaining companies both proposed the same solution—*DarkTrace*—and therefore they were invited to present to representatives from the Brigade.

4.9. BT and Insight Direct (the two companies that *DarkTrace* were invited to present on behalf of) are on different frameworks. BT are on the Pan-London ICT Framework and Insight Direct are on the CCS framework. Both companies were evaluated using the same evaluation criteria. This was possible because the Pan London ICT Framework does not stipulate any evaluation criteria, the evaluation guidance of the CCS framework was followed and used for all tenderers.

4.10. On quality, both companies proposed the *DarkTrace* product were evaluated and awarded the same scores. The quality elements of their bids were exactly the same as they had been written by a representative of *DarkTrace*. Therefore, the only difference in score was in relation to the price submitted, leading to the recommendation of BT Global Services as the successful tenderer.

Strategic drivers

4.11. Page 55 of the London Safety Plan says: *"Digital technologies offer all public services, including the fire and rescue service, the opportunity to deliver better outcomes for local residents, businesses and communities. London Fire Brigade's strategy for digital transformation sets out a vision and the practical steps needed to move the Brigade toward a digital future over the next ten years"*.

4.12. Page 22 of the Brigade's strategy for digital transformation referred to in the London Safety Plan, *'LFB in a Digital World'*, says *"During the life of this strategy we will complete … [the implementation of] a cyber defence system."*

4.13. The proposal to the Commissioner in report LFC-0152 is a key delivery requirement for these strategic drivers.

5. Financial comments

5.1 Report LFC-0152 to the Commissioner recommends that the successful tender for a cyber defence system is accepted at an annual revenue cost of £106,000, with a contract life of two years. This is £22,000 higher annually than the revenue budget of £84,000, agreed in the 2018/19 Budget Report. If approved, the budget will be increased from 2020/21 through the Medium-Term Forecast. However, there will potentially be a pro-rated overspend against the monthly projections in 2019/20 that will be reported on as part of the regular financial position reports. The expenditure is to be funded through sums available to the Commissioner. 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 London Fire Commissioner (the "Commissioner") 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 Commissioner 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 Commissioner would require the prior approval of either the Mayor or the Deputy Mayor for Fire and Resilience (the "Deputy Mayor").

6.3. Paragraph (b) of Part 2 of the said direction requires the Commissioner 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…".

6.4. The Deputy Mayor's approval is accordingly required for the Commissioner for such expenditure on the cyber defence system.

6.5. The procurement of the cyber defence system is consistent with the Commissioner's power under section 5A of the Fire and Rescue Services Act 2004 to procure services they consider appropriate for purposes incidental to their functional purposes.

6.6. Under section 2(1) of the Policing and Crime Act 2017, the Commissioner has a duty to keep under consideration whether entering into a collaboration agreement with one or more other relevant emergency services in England could be in the interests of the efficiency or effectiveness of that service and those other services.

6.7. The General Counsel to the Commissioner also notes that the cyber defence system has been procured in compliance with the Public Contracts Regulations 2015.

6.8. In taking the decisions requested, the Deputy Mayor must have due regard to the Public Sector Equality Duty - namely the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by the Equality Act 2010 and to advance equality of opportunity and foster good relations between persons who share a relevant protected characteristic (race, disability, gender, age, sexual orientation, religion or belief, pregnancy and maternity and gender reassignment) and persons who do not share it (section 149 of the Equality Act 2010). To this end, the Deputy Mayor should have particular regard to section 3 (above) of this report.

Appendices and supporting papers:

LFC-0152 – 'Cyber Defence System: Acceptance of Tender'

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 either be published 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? YES
If YES, for what reason: The commercial interests of the Commissioner require the deferral of publication of the Deputy Mayor's decision until after the contract award and subsequent cooling off period proposed by report LFC-0152 to the Commissioner.

Until what date: 1 September 2019

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 – NO

ORIGINATING OFFICER DECLARATION:	Drafting officer to confirm the following (✓)
Drafting officer Andrew Nathan has drafted this report with input from the LFC and in accordance with GLA procedures and confirms the following:	✓
Assistant Director/Head of Service Tom Middleton 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.	✓
Corporate Investment Board This decision was agreed by the Corporate Investment Board on 10 June 2019	

EXECUTIVE DIRECTOR, RESOURCES:
I confirm that financial and legal implications have been appropriately considered in the preparation of this report.

Signature M. D. Mc **Date** 10.6.19