LONDON FIRE BRIGADE

Decision title

# Cyber Defence System: Acceptance of Tender

Recommendation by
Chief Information Officer

Decision Number
LFC-0152-D

Protective marking: **OFFICIAL - Sensitive**
Publication status: Published with redactions


## Summary
This report seeks 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.


## Decision
The London Fire Commissioner (LFC) approves the acceptance of the preferred tender for the supply of a Cyber Defence System from the supplier and for the value set out in the confidential appendix B to this report. The contract value is £ 212k over two years.

**Dany Cotton QFSM**
London Fire Commissioner

Date 21/6/19

| Access to Information – Contact Officer | |
|---|---|
| **Name** | Steven Adams |
| **Telephone** | 020 8555 1200 |
| **Email** | governance@london-fire.gov.uk |

LONDON FIRE BRIGADE

Report title

# Cyber Defence System: Acceptance of Tender

| Report to | Date |
|---|---|
| Commissioner's Board<br>Fire and Resilience Board<br>London Fire Commissioner | 27 March 2019<br>9 April 2019 |
| **Report by** | **Report number** |
| Chief Information Officer | LFC-0152 |

Protective marking: **OFFICIAL - Sensitive**

Publication status: Published with redactions


## Summary

This report seeks 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.


## Recommendations

That the London Fire Commissioner (LFC) approves the acceptance of the preferred tender for the supply of a Cyber Defence System from the supplier and for the value set out in the confidential appendix B to this report. The contract value is £ 212k over two years.

## Introduction

1. The purchase of a cyber defence system was included as a growth item (G08) for 'security monitoring software' as part of the 2018/19 budget agreed by the former LFEPA (FEP2825).

2. The paper also explains the recent and current cyber threat environment and why a cyber defence system is needed. This paper recommends the acceptance of a tender for a Cyber Defence System to protect the Brigade ICT infrastructure from cyber attacks.

## Background

3. In recent years, the security threat posed to organisations around the globe from cyber attacks, malware and associated threats, has increased exponentially. Most of us will remember only too well the "WannaCry" ransomware attacks that took place last year.

4. 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.

5. 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 dollars of damage in the 2000s.

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

7. 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 weekend 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.

8. 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).

9. However, as the nature and frequency of threats evolve and increase, it is clear that we need 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.

## Security information and event management systems (SIEM)

10. In determining its requirements, the Brigade initially identified a need to deploy a security information and event management system (SIEM; pronounced 'sim')'. 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 predetermined 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.

11. 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.

12. 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

13. 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.

14. 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

15. 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.

16. 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.

17. 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.

18. The 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.

## The way forward

19. 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.

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

## Potential collaboration

21. The Chief Information Officer has spoken to colleagues within the GLA group and at other fire and rescue services about its requirements, and the opportunities for collaboration. Visits were undertaken to TfL to see their security monitoring operation arrangements in action. TfL were very helpful and it was useful to understand their setup and approach. The system that they use is dedicated to TfL use, and demands a large team to analyse the information produced, which is

the scenario that the Brigade are trying to avoid. There are no obvious collaboration opportunities with them or the other GLA functional bodies or other fire and rescue services at present.

22. We have consulted with the MPS over their product selection in this area. The MPS have selected an alternative product which will better cope with the larger traffic volumes in their IT estate but otherwise they did consider Darktrace to be a viable alternative and were confident that it would scale suitably for the LFB estate.

## Procurement action

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

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

    - Crown Commercial Service (CCS) Technology Products 2 (RM 3733, Lot 3), and
    - Pan London ICT Framework (Lot 4).

25. 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 invitation to participate to ensure compliance with the Procurement Regulations.

26. An *Invitation to Participate* was published on 3 December 2018 to the 19 companies listed on 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. The evaluation was carried out in two stages.

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

27. The outcomes of the two stage tender evaluation process is outlined in the confidential appendices A and B.

### Finance comments

28. This report recommends that the successful tender for a cyber defence system is accepted at an annual 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 an overspend in 2019/20 that will be reported on as part of the regular financial position reports

## Workforce comments

29. No staff side consultation is proposed on this report.

## Legal comments

30. 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.

31. 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").

32. 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...".

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

34. 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.

35. 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.

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

## Sustainability implications

37. There are no specific sustainability implications arising from this proposal.

## Equalities implications

38. The Public Sector Equality Duty applies to the London Fire Brigade when it makes decisions. The duty requires us 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) c) Foster good relations between people who share a protected characteristic and those who do not including tackling prejudice and promoting understanding.

39. The protected characteristics are age, disability, gender reassignment, pregnancy and maternity, marriage and civil partnership, race, religion or belief, gender, and sexual orientation. The Act states that 'marriage and civil partnership' is not a relevant protected characteristic for (b) or (c) although it is relevant for (a).

40. An equalities impact 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 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. In fact, the key intended purpose of the software is to strengthen and protect individuals from a cyber security attack.

**NOT FOR PUBLICATION**

**Freedom of Information Act 2000: 43 Commercial interests**

(2) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it).

**Appendix A**

# Procurement, tender evaluation and outcomes

[redacted]

[redacted]

**Appendix B**

# Tenderer scoring outcomes – Stage 1

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted]% |