LONDON FIRE BRIGADE

Report title

Cyber Defence System: Contract Extension

Report to	Date
Corporate Services Board Deputy Mayor's Fire and Resilience Board London Fire Commissioner	8 December 2020 19 January 2021
Report by	**Report number**
Chief Information Officer	LFC-0474y

Protective marking: **OFFICIAL - Sensitive**
Publication status: Published with redactions
If redacting, give reason: Commercially sensitive information

Executive Summary

This report seeks authority to extend the contract with BT in accordance with its terms for the provision of the cyber defence system for two further years when the contract expires in July 2021. The original procurement provided an opportunity to enter into a contract for an initial two-year period and an option for the London Fire Commissioner to extend by a further two years. However, the additional two-year extension was never requested as part of the original approval (LFC-0152-D). Due to the complexity and resource implications associated with the implementation and configuration of this system, our intention was always to run the system for four years (subject to satisfactory performance in the first two years).

Recommended decisions

For the Director of Corporate Services
That the Director of Corporate Services decides that the Assistant Director Technical & Commercial be authorised to extend the existing cyber defence contract with BT for a period of not more than 24 months at a cost of not more than £ 214,286.00[1].

Introduction and Background

1. In July 2019, the London Fire Commissioner (LFC) accepted a tender (LFC0152-D) from BT for the purchase of a cyber-defence system at a cost of £212K for a two-year period with an option for the LFC to extend for a further two years. Unfortunately, the authority to commit expenditure for the additional two years available under the framework call off, was not sought at the time. This report addresses this issue and seeks agreement to expenditure to allow extension of the existing contract in accordance with its terms.

2. As outlined in the original decision, the security threat posed to organisations around the globe from cyber-attacks, malware and associated threats, has increased exponentially. Most will remember the "WannaCry" ransomware attacks that took place in 2017.

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 dollars of damage in the 2000s.

4. The Brigade itself was unaffected by the WannaCry ransomware due to the efforts of ICT staff who worked 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.

5. There is no reason to believe that the threat to systems around the world will do anything other than increase. Some 88% of UK companies have suffered a data breach in the last 12 months (Source: carbon black reports) and in October of this year , the London Borough of Hackney was subject to a cyber-attack that caused massive disruption to council operations and is the subject of a large scale cyber clean-up operation. 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, it is essential that we maintain our existing cyber defence capability.

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 (NCSC) and potentially seeking accreditation against the Cyber Essential Plus standard (which requires external accreditation). Our initial gap analysis got under way in November 2020.

Alternative Options Considered

7. The alternative to not seeking to use the contract extension available would be to initiate a new procurement and either re-procure the existing product or select an alternative, depending upon the result of the tender evaluation. The procurement, selection and most notably installation of a cyber defence product is a very substantial undertaking and demands extensive resource allocation from the Brigade's ICT security team.

8. As we have learnt from our direct experience with installing the cyber defence system, the workload does not stop once the product is installed. Any product has to take time to learn about the way the infrastructure within the organisation operates, its unique operating environment. This phase of post installation "learning" can be very time consuming as staff work with the system to identify "false positives" and adjust sensitivity levels to ensure that the Brigade's business as usual and critical operations are not impacted.

9. At present the cyber threat within the UK is increasing and it is acknowledged that the cyber defence system provided is a leading cyber defence system with around 4000 customers world-wide. The product has worked well since its introduction and has recently taken action to quarantine devices when suspect "malware" was detected.

10. A number of discussions were held with both TfL and the Metropolitan Police in relation to collaboration opportunities, prior to the current system being selected. No collaboration opportunities were identified at the time. However, given that our strong preference is to extend the existing contract for a further two years as the contract allows, we would seek to engage with partners in the GLA and in the wider Fire Service, prior to initiating the full re-procurement prior

to July 2023, which would allow sufficient time to discuss the alignment of contract expiry dates and any potential aggregation of requirements (subject to this report being authorised).

11. Taking the above points into consideration it is our view that the best course of action at this time is to extend the contract for a further two years, rather than initiate re-procurement.

Objectives and Expected Outcomes

12. The objective of this report is to seek authorisation to extend the existing contract with BT for use of the cyber defence system provided by two years. This will allow the Brigade to continue using the system up to the end of July 2023.

Impacts

13. There will be no impact upon Brigade if the contract is extended to run for two years from its expiry date on July 2021, as long as the necessary approvals for the next procurement are in place prior to contract expiry.

14. If authorisation to extend the contract is not provided, a full re-procurement will need to be undertaken which would incur additional procurement and potential further installation costs. In this case a new report will need to be submitted through the governance process.

15. If a new procurement is to be undertaken, there will be a significant implication for ICT security staff. The original plan was to use the existing system for a period of four years. As referenced above, authorisation was only sought and given for the initial period of two years. This will mean amending the ICT work plan with consequential impacts upon other projects.

Equality Impact

16. The London Fire Commissioner and decision takers are required to have due regard to the Public Sector Equality Duty (s149 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.

17. 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.

18. 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, Sexual orientation.

19. The Public Sector Equality Duty requires us, in the exercise of all our functions (i.e. everything we do), to have due regard to the need to:

    (a) Eliminate discrimination, harassment and victimisation and other prohibited conduct.
    (b) Advance equality of opportunity between people who share a relevant protected characteristic and persons who do not share it.
    (c) Foster good relations between people who share a relevant protected characteristic and persons who do not share it.

20. 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:

    (a) remove or minimise disadvantages suffered by persons who share a relevant protected characteristic where those disadvantages are connected to that characteristic;
    (b) 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;
    (c) 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.

21. 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.

22. 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—

    (a) tackle prejudice, and
    (b) promote understanding

    .

23. An equalities impact was carried out as part of the original procurement. This indicated 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

Procurement and Sustainability

24. The LFC awarded the contract to BT by way of mini competition utilising the Pan London ICT Framework Lot 4. The contract is for an initial term of two years and commenced on 18 July 2019. The contract also includes an optional further extension of two years if notice is given prior to expiry of the contract. The current expiry date is 17 July 2021, prior to enacting any further period of extension and with the last date to notify the supplier of the intention to extend being 17 April 2021. Extending the contract would see it terminate on 17 July 2023.

25. A price review is due on the anniversary of the contract, which will be in accordance with the indices referenced in the terms and conditions, which is CPI (Consumer Price Inflation). According to the Office for National Statistics (ONS) the CPI is currently 0.7%. BT have confirmed that should the extension be agreed the price increase requested will be 0.7%. This has been included in the total figure in the Recommended decisions above.

26. Consideration of Responsible Procurement requirements will be undertaken as standard process as part of the future re-tender. Responsible Procurement performance of the supplier, BT includes:

    i. Compliance with the Modern Slavery Act with a published Statement;
    ii. a Prompt Payment Code signatory and compliant with the Code's target of 95%;
    iii. operating an Environment Management System certified to ISO 14001; and

iv. reporting an average gender pay gap of one pence.

Responsible Procurement performance of the cyber defence product manufacturer includes:

i. A large supplier based on turnover;
ii. a published Modern Slavery Statement, although it is now out of date;
iii. reporting an average gender pay gap of 8.8% in favour of men; and
iv. no submitted reports on prompt payment performance.

Strategic Drivers

27. The extension of the existing cyber defence contract will allow the Brigade to continue to ensure that a both operational and FRS staff are able to carry out their roles, to serve and protect the people of London, by ensuring that all Brigade activities are able to continue, safe from attack by hostile actors.

Workforce Impact

28. There are no plans to consult further in respect of this report.

Finance comments

29. This report requests a two year extension to the existing Darktrace cyber-defence system contract, which expires in July 2021, at a cost of up to £214,286. This extension is provided for under the contract which was previously awarded in 2019. Under the terms of the contract a price review takes place on the anniversary of the contract, and the agreed increase is 0.7%, which has been included in the total cost figure. The funding for the contract is contained in the current ICT (Server and Cloud - Software Off-the Shelf) budget.

Legal comments

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.

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").

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…".

4. The Deputy Mayor's approval is accordingly required for the Commissioner for such expenditure on the extension of the cyber defence system contract.

5. The original 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. 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.

30. The General Counsel also notes that the cyber defence system was procured in compliance with the Public Contracts Regulations 2015, but that the two year optional contract extension and the expenditure to cover the contract extension were inadvertently omitted from the approvals sought before the award of the contract.

List of Appendices

Appendix	Title	Protective Marking
1.	None	