LONDON FIRE BRIGADE

Report title

Network Security Licencing and Support Renewal

Report to	Date
Corporate Services Board Commissioner's Board Deputy Mayor's Fire and Resilience Board London Fire Commissioner	20 July 2021 25 August 2021 12 October 2021

Report by	Report number
Chief Information Officer	LFC-0581y

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

Executive Summary

Over the past seven years, in response to ever increasing cybersecurity and viral threats including ransomware, the network security infrastructure has grown significantly to include a number of specialist products to detect and prevent malicious activity.

The LFB network security environment now includes a variety of components designed to secure and protect the LFB network. These products combined, protect the various solutions LFB rely on, including LFB infrastructure, wired and wireless networks, hosted voice solutions, internet connectivity and the mobilising environment.

The contract to support these devices has recently been extended for the final time and will need to be re tendered for support to continue after February 2022. The scope of the contract will include not only hardware and software support for the relevant network security equipment, but also the required licences to ensure the security products are up to date and effective.

This report seeks authority to retender the support and licencing of these products and award a new contract for support of these products.

Recommended decision

For the London Fire Commissioner

The London Fire Commissioner agrees to commit revenue expenditure of up to [redacted] to procure a new support contract for network security and licensing for up to a five-year period from February 2022.

Introduction and Background

1. The LFB network Infrastructure incorporates a security environment which has grown significantly over the last seven years. Initially it was introduced to separate the wireless and wired networks. This infrastructure has been developed and refined to meet the increasing digital threat and to comply with the ever-changing government security requirements designed to keep organisations safe from malicious threats.

2. The present security environment incorporates identity services engine (ISE), firepower management centre (FMC) and a variety of Cisco adaptive security appliances (ACS), which are next generation firewalls incorporating anti malware protection.

3. A Firewall is a network security device that monitors, and filters incoming and outgoing network traffic based on an organisation's security policies. At its simplest, a firewall is the security barrier that sits between a private internal network and the outside world. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous or malicious traffic out.

4. The current setup was introduced in 2017 and is an ongoing solution which changes with the developments in technology and threats. The original tender involved the purchase, licencing, and support of the equipment. This contract has been extended for the final time (3+2) and a new contract is required for February 2022 to ensure support and licencing can continue uninterrupted.

5. Presently the environment includes 5 ISE units, 1 FMC and 14 adaptive security appliance (ASA) Firewalls of varying models.

   These Firewalls and security solutions are used for the following purposes:

   - Control and mobilising system (CAMS) firewalls. Capita environment segregation and security.
   - Azure Firewall. Cloud solution.
   - Wireless LAN (WLAN) Firewalls. Wireless/wired network segregation.
   - Identity service engine.
   - ISP firewalls (internet connection). (demilitarised zone - DMZ)/ISP sites.)
   - ISE Lite. Guest wireless access.
   - Firepower management centre (FMC). IPS and traffic management /analysis.
   - PDA firewall. Control PC segregation, virtual private network (VPN).
   - Voice firewalls. Hosted voice solution.
   - Hot spot wireless firewall. Guest access.
   - Sawyer Street firewall. Car park utilities.

6. The LFB network has over time become increasingly more complex and critical to the operational effectiveness of the Brigade. The essential purpose of re tendering for support is to ensure all security items within the environment are kept up to date. Specifically, this includes software versions, patches, licensing, virus updates and that the policies on the ASAs are in line and fit for purpose. Below is a more in-depth explanation of the suite of products used to protect the LFB network.

7. Cisco ISE (identity service engine) is a solution that provides context-aware identity management and determines whether users are accessing the network on an authorised, policy-compliant device. It can establish the user's identity, location, and access history, which can be used for compliance and reporting. It can also assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on) and grant authenticated users with access to specific parts of the network or applications.

8. Cisco ISE is currently being developed to ensure only LFB laptop builds and devices can join the network and will protect the network points at LFB premises. This protection of network points will only allow LFB devices to plug into the network. Any external device that is not recognised as an LFB device will not be able to access any network resources. This software protection of the network ports is essential if Fire Stations are to be opened to members of the public. Please note this is not a physical security method, but a software solution.

9. The Cisco ASA Firewalls LFB use are industry leading and are not only used to protect LFB from the outside world, but also used to segregate the LFB network from the mobilising network. This segregation between Capita and LFB is designed to protect both environments whilst still allowing essential communications between the two networks.

10. Firewalls are also used to connect LFB to the external world, via the internet service provider (ISP). These Firewalls ensure activities such as remote access, web browsing, email, MS 365 and other critical activities are safe and secure. They are also an integral part of the wireless network, and as LFB staff return to union street and other office-based locations, will become an essential to enabling modern, flexible working.

11. Intrusion prevention system (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application or can potentially access the rights and permissions available to the compromised application.
    The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.

12. Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Without the up to date signatures the licencing provides, the IPS solution becomes increasingly less effective over time.

13. FMC (firepower management centre) is the administrative centre for Cisco security products, running on a number of different platforms. It provides complete and unified management of firewalls, application control, intrusion prevention, Web site filtering, and advanced malware protection. The Cisco firepower management centre provides extensive intelligence about the users, applications, devices, threats, and vulnerabilities, that exist in the network. It also uses this

information to analyse the network's vulnerabilities. It provides recommendations on what security policies to put in place and what security events you should investigate.

Costs

The exact cost may vary due to several factors including general market conditions and exchange rates, but estimates are based on current market costs of the equipment as set out in the table 1:

TABLE 1: COSTS		
	12 Months Cisco SMARNET and Licensing Hardware support for smartnet total care (SNTC) 8*5*next busines day (NBD) short message service (SMS-1) Software support service- (SWSS) UPGRADES SMS-1 [1]	[redacted]
Expected Annual Cost		[redacted]

A detailed current cost breakdown is set out in appendix 1, Table 2:

14. As part of the current ICT environment the above sums are included in the current approved revenue budgets. The approval sought includes a contingency sum of [redacted] over the life of the contract to allow for fluctuations in exchange rates and potential changes to the security architecture arising from organisational change. This sum can also be met from existing revenue budgets.

Alternative Options Considered and Consultation

15. An alternative option is to continue using the existing equipment with no hardware support. Whilst the majority of the hardware has redundancy built in, and in theory parts can be purchased by LFB through a number of suppliers if something fails, this would leave the LFB with an unacceptable level of risk, particularly in respect to our mobilising environment. Having a contracted and agreed service level agreement of an eight hour fix in place relating to service restoration and fault resolution, minimises the risk and possible downtime that may result from a hardware failure.

16. Without the correct licencing, the firewalls will not receive either security or software updates. Whilst they can still be used, they would not be aware of any new possible security threats and become less effective as time goes on due to having out of date signatures. Cyber security and the threats to an organisation become more sophisticated and are ever evolving. It becomes a constant battle to stay ahead of the threat actors, and with no licence updates or support, the security environment and its defences will become weakened within a very short space of time.

---

redact

Objectives and Expected Outcomes

17. The objective of this report is to secure authorisation to enter into a support contract for network security and licensing. This will enable the LFB to ensure ICT systems are secured against all forms of cyber-attack and malicious activities. Essential security defences that are no longer able to receive security updates or have hardware support in the event of a failure, can pose a significant threat to the LFB infrastructure, including the mobilising environment.

Impacts

Equality Impact

18. 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.
19. 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.

20. 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.

21. 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.

22. 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 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.

23. 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.

24. 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 to the need to
    1. tackle prejudice, and
    2. promote understanding.

25. An Equality Impact Assessment (EIA) has not been completed for this report as there will be no impact on any groups with protected characteristics. The outcome of the procurement will be a replacement of network and security products and licenses and will therefore be transparent to users.

Procurement and Sustainability

26. Use of the TfL ICT Resellers Framework was considered as a potential route to market. Contact has also been made with the GLA Collaborative Procurement Team to seek interest from other functional bodies who may have a similar requirement. To date no expressions of interest have been received. This framework has now been discounted as there are others that offer more favourable commercials.

27. Other potential collaborative procurement routes that have been identified to date are the use of the Crown Commercial Service (CCS) Technology Services 3 Framework, and the NHS London Procurement Partnership (LPP) Information Management & Technology (IM&T) Framework.

28. Technology Services 3 offers public sector buyers a flexible and compliant way to source all their technology product needs. The framework is due to go live on 14 July 2021. 64% of the 253 suppliers on this framework are SMEs. The UK public sector and their associated bodies and agencies, including the voluntary sector and charities, can use this framework.

29. LPP has established the Information, Management & Technology (IM&T) Framework which consists of suitably experienced, capable, qualified and resourced suppliers available for use by NHS trusts, clinical commissioning groups, GP services and other health and social care providers within the United Kingdom and Northern Ireland, as well as local authorities and third sector organisations. The purpose of the framework is to provide a compliant route to market for each of the initiatives.

30. When tendering for this service on previous occasions the CCS frameworks were used, however they often result in limited tender responses. The LLP framework offers some additional suppliers that have not previously been invited to tender and in order to encourage maximum market engagement it is likely that this framework will be the preferred route to market. A firm decision cannot be made at this point in time as all of the documents for the CCS framework are not currently available so that a full analysis can be carried out. From previous experience the LLP framework also offered more favourable commercials which again will need to be assessed to ensure that best value is achieved.

31. Any new procurement activity will need to be undertaken in line with the GLA group Responsible Procurement policy. At present no specific sustainability implications have been identified in relation to this procurement.

Strategic Drivers

32. The strategic driver for this proposal would align with the strategic pillars 'Seizing the future' and 'Delivering Excellence' and in particular would support the aims – *'constantly improving effectiveness of our service'* and *'improved execution'*, for the reasons outlined in this paper.

Workforce Impact

33. There is no foreseeable impact on the workforce from continuing to have a supported network security environment. There would however be an impact on workforce resources and skillsets if the support agreement cannot be renewed, and LFB ICT staff needed to provide security without the relevant systems and manufacturer support that would be required.

Finance comments

34. This report recommends that revenue expenditure of up to [redacted], including a [redacted] contingency, is agreed to procure a new support contract for network security and licensing for up to a five-year period. The cost of this will be met from within existing ICT department budgets.

Legal comments

35. 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.

36. 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").

37. 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…".

38. The Deputy Mayor's approval is accordingly required for the Commissioner to commit to expenditure the sums set out in this report.

39. The statutory basis for the actions proposed in this report is provided by section 5A of the Fire and Rescue Services Act 2004, under which the London Fire Commissioner, being a 'relevant authority', may do 'anything it considers appropriate for the purposes of the carrying out of any of its functions'.

40. The General Counsel also notes that the proposed procurement route for this service is in compliance with the Public Contracts Regulations 2015 undertaken in line with the Commissioner's policies and the GLA group Responsible Procurement policy.

List of Appendices

Appendix	Title	Protective Marking
1.	Table 2 – Detailed Costs	Official sensitive

Appendix1

Table 2: Detailed costs

Item	Description	Qty	Total
CON-ECMU-R-ISE-VM	SWSS UPGRADES Cisco Identity Services Engine VM (eDelivery)	2	[redacted]
CON-SNT-A45FPK9	SNTC-8X5XNBD ASA 5545-X with FirePOWER services, 8 gigabit ethernet (GE),	2	[redacted]
CON-SNT-A25FPK9	SNTC-8X5XNBD ASA 5525-X with FirePOWER Services, 8GE,	4	[redacted]
CON-ECMU-VMWSW10	SWSS UPGRADES Cisco firepower management center,(VMWare)	1	[redacted]
CON-SNT-ASA556F9	SNTC-8X5XNBD ASA 5516-X with FirePOWER services, 8GE	2	[redacted]
CON-ECMU-R-ISE-VM	SWSS UPGRADES Cisco Identity Services Engine VM (eDelivery)	1	[redacted]
L-AC-APX-1Y-S1	Cisco AnyConnect Apex License, 1YR, 25-99 Users	25	[redacted]
L-ASA5585-20-TA1Y	Cisco ASA5585-20 FirePOWER IPS 1YR subscription	4	[redacted]
CON-SNT-ASA5506K	SNTC-8X5XNBD ASA 5506-X with FirePOWER services, 8GE,	1	[redacted]
L-ASA5516-TAMC-1Y	Cisco ASA5516 FirePOWER IPS, advanced malware protection (AMP) and uniform resource locators (UR)L 1YR Subs	2	[redacted]
L-ASA5525-TAMC-1Y	Cisco ASA5525 FirePOWER IPS, AMP and URL 1YR subscription	4	[redacted]
L-ASA5545-TA-1Y	Cisco ASA5545 FirePOWER IPS 1YR subscription	2	[redacted]
CON-SNT-SSPFP209	SNTC-8X5XNBD ASA 5585-X FirePOWER SSP-20, with 8GE,	4	[redacted]
CON-SNT-SNS3515K	SNTC-8X5XNBD Small Secure Network Server for ISE lApplication	2	[redacted]

L-ASA5545-TA-1Y	Cisco ASA5545 FirePOWER intrusion prevention system (IPS) 1YR subscription	2	[redacted]
L-ASA5585-20-TA1Y	Cisco ASA5585-20 FirePOWER IPS 1YR subscription	4	[redacted]
L-ASA5525-TAMC-1Y	Cisco ASA5525 FirePOWER IPS, AMP and URL 1YR subscription	4	[redacted]
L-AC-APX-1Y-S1	Cisco AnyConnect Apex License, 1YR, 25-99 Users	25	[redacted]
L-ASA5516-TAMC-1Y	Cisco ASA5516 FirePOWER IPS, AMP and URL 1YR subscription	2	[redacted]
TOTAL			[redacted]