

REQUEST FOR DMPC DECISION – DMPCD 2016 108

Title: ICT Security Procurement

Executive Summary:

This paper requests approval to extend the ICT Service Integration and Management (SIAM) contract with Atos for 48 months from December 2016 to allow implementation of a security services solution and approve funding of £6.24m (£438k capital plus £5.76m revenue) over the extended contract period.

Recommendation:

The DMPC is asked to:

1. Approve additional funding of £6.24m (£438k capital plus £5.76m revenue).
2. Approve the extension of the SIAM contract with Atos for 48 months.

Deputy Mayor for Policing And Crime

I confirm I have considered whether or not I have any personal or prejudicial interest in this matter and take the proposed decision in compliance with the Code of Conduct. Any such interests are recorded below.

The above request has my approval.

Signature

Sybil Under

Date

08/12/2016

PART I - NON-CONFIDENTIAL FACTS AND ADVICE TO THE DMPC

Decision required – supporting report

1. Introduction and background

- 1.1. In 2015, Atos was appointed as the new SIAM partner. Cap Gemini had been providing an interim ICT security service for the MPS. The contract with Cap Gemini expired on the 31st October 2016, however it has been extended on a month by month basis to enable the service to continue. The current monthly service cost with Cap Gemini is £116,833. The proposal from Atos is for a monthly cost of £120,000 per month with additional functionality.
- 1.2. This is a foreseen extension of the SIAM/Towers arrangement as stated in Schedule 1 of the SIAM/Tower contract.

2. Issues for consideration

- 2.1. These are discussed in Part 2.

3. Financial Comments

- 3.1. The revenue costs are unfunded in the current financial year and also in future years. The MPS is proposing to use potential savings from the fixed line telecoms contract which are estimated to be in excess of £1m a year to fund the 2016/17 revenue costs of £480,000. For future years costs from 2017/18, these will be funded from a combination of ongoing savings in the fixed line telecoms costs and rationalisation of applications resulting in a total estimated saving of £2m per annum.
- 3.2. Further details regarding the revenue funding is contained in the Part 2.
- 3.3. The capital costs of £483,000 can be met from existing budget provision.

4. Legal Comments

- 4.1. These are discussed in Part 2 – Commercial section.

5. Equality Comments

- 5.1. There are no direct equality or diversity implications arising from this report

6. Background/supporting papers

- 6.1. Appendix 1.

Public access to information

Information in this form is subject to the Freedom of Information Act 2000 (FOIA) and other legislation. Part 1 of this form will be made available on the MOPAC website within 1 working day of approval. Any facts/advice/recommendations that should not be made automatically available on request should not be included in Part 1 but instead on the separate Part 2 form. Deferment is only applicable where release before that date would compromise the implementation of the decision being approved.

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 as likely to be exempt from disclosure under the FOIA should be in the separate Part 2 form, together with the legal rationale for non-publication.

Is there a **part 2** form -YES

If yes, for what reason: EXEMPT under Article 2(2)(a) of the Elected Local Policing Bodies (Specified Information) Order 2011.

ORIGINATING OFFICER DECLARATION:

	<i>Tick to confirm statement (✓)</i>
Head of Unit: The Head of Strategic Finance and Resource Management has reviewed the request and is satisfied it is correct and consistent with the MOPAC's plans and priorities.	✓
Legal Advice: The MPS legal team has been consulted on the proposal.	✓
Financial Advice: The Head of Strategic Finance and Resource Management has been consulted on this proposal.	✓
Equalities Advice: No Equality and Diversity issues identified.	✓

OFFICER APPROVAL**Chief Executive Officer**

I have been consulted about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. I am satisfied that this is an appropriate request to be submitted to the Deputy Mayor for Policing and Crime.

Signature R. Lawrence

Date 7/12/16

SIAM Security Services

Investment Advisory Board – 22nd November 2016

Report by Angus McCallum on behalf of the Deputy Commissioner

EXECUTIVE SUMMARY

This paper articulates the capital investment of £483,000 to implement the Atos solution for enhanced security across the SIAM / Towers model. It also articulates the ongoing revenue cost of £5.76M to replace the existing Cap Gemini arrangement. This also seeks approval to proceed with a foreseen extension of £6.24m (£483K capital plus £5.76m) bringing the SIAM Tower Contract value to £64.19m

A. RECOMMENDATIONS - That

1. The Deputy Mayor for Policing and Crime approves expenditure of £120,000 per month for the remaining duration of the SIAM contract (48 months from Dec 2016) totaling £5.76m.
 - This equates to an increase of £1.4m per annum against an average £9m per annum (including Solution Delivery Integration and Management).
 - If the project is approved 2016-17 revenue requirements of £480k will be funded from savings to be made in the fixed line telecoms contract estimated to exceed £1m in that year. Costs from 2017-18 onwards will be funded by a combination of ongoing savings in fixed line telecoms costs and rationalisation of applications resulting in a total estimated saving of £2m per annum

B. SUPPORTING INFORMATION

1. This paper concerns the implementation of a security services solution across the Service Integration and Management (SIAM) / Towers model. Currently MOPAC/MPS have extended a contractual arrangement with Cap Gemini on a monthly renewable basis to provide continuity of service, it is accepted that at current levels this does not provide an adequate and future proofed solution. To move to a SIAM managed solution requires capital investment so that the appropriate tools are in place. This is a foreseen extension to the SIAM /Towers arrangements as articulated in Schedule 2.1 of the SIAM Tower contract.
2. The current extended legacy arrangement with Cap Gemini, which had a revenue cost of £116,833 per month, expired on the 31st October 2016, but this has been extended on a month by month basis beyond October 2016; the alternative solution and proposal from Atos is for a revenue cost of £120,000 per month for a vastly optimized service, providing the MPS with appropriate security services for today and the future.
3. This is in line with the One Met Model and is part of Programme 10, Enhancing Digital Policing for 2020.

C. OTHER ORGANISATIONAL & COMMUNITY IMPLICATIONS

Equality and Diversity Impact (mandatory)

1. There are no equality or diversity issues arising from this proposal.

Financial Implications / Value for Money (mandatory)

1. It is proposed that the expenditure on this project, if approved, will be financed by savings in the fixed line telecoms contract estimated at £1m p.a. in 2016-17 and later years, and applications rationalisation estimated at a further £1m p.a. in 2017-18 and beyond.

Legal Implications (mandatory)

1. No Significant Legal implications

Consultation undertaken (mandatory)

- 1.

Consultation grid

The following people have been consulted internally in the production of this Business Justification and their opinions incorporated. In addition to those consulted below, Lynda McMullan, Director of Commercial and Finance and Angus McCallum, CIO have been consulted and reviewed the proposal.

Directorate / Dept.	Name & Job Role	Rank / Grade	Date Assured
Procurement	Sheldon Mydat / Karen Hendry	S	12/09/2016
DP	Pete Trainer – DP Service Delivery Director	SPG3	14/09/2016 & 10/11/16
HR	N/A		
Legal (DLS)	Prit Mandair – Legal		08/09/2016
Property	N/A		
Finance Business Partners	Pat Woodhouse – Finance		12/09/2016 & 10/11/16
Health & Safety	N/A		
DCFD	N/A		

Risk (including Health and Safety) Implications (mandatory)

1. No risks identified.

Real Estate and Environmental Implications (if relevant to the subject)

1. No Real Estate or Environmental implications identified.

Business Justification

SIAM Security Services

Capital and Revenue proposal (SMP funded capital)

Investment Advisory Board

22 November 2016

Freedom of Information Act Publication Scheme

Protective Marking

Commercial – not Protected (with the exception of Part 2 which is exempt - commercially protected)

Publication Scheme Y/N

See above

Freedom of Information Act Publication Scheme

Title	Security services SIAM / Towers Ecosystem
Version	0.6
Summary	This paper articulates the capital investment of £483,000 to implement the Atos solution for enhanced security across the SIAM / Towers model. It also articulates the ongoing revenue cost of £5.76M to replace the existing Cap Gemini arrangement. This also seeks approval to proceed with a foreseen extension of £6.24m (£483K capital plus £5.76m) bringing the SIAM Tower Contract value to £64.19m
(B)OCU or Unit, Directorate	Digital Policing
Author	Mark McLeod , Director Service Management (SIAM) & Data Centres
Review Date	
Date Issued	November 2016

Version History

Version	Date	Additions/Modifications	Prepared/Revised by
0.1	10/8/2016	First draft	Mark McLeod
0.2	12/9/2016	Financial	Pat Woodhouse
0.3	12/9/2016	Commercial	Sheldon Mydat
0.4a	14/09/2016	Commercial	Sheldon Mydat
0.4b,c,d	20/09/16	Financial	Pat Woodhouse
0.4e	22/09/16	Commercial	Katherine King
0.5	10/11/2016	DP and FBP	Pete Trainer & Pat Woodhouse
0.6	11/11/2016	Finance	Pat Woodhouse / Ian Percival

Internal Consultation & Assurance

The following people have been consulted in the production of this Business Justification and their opinions incorporated.

Directorate / Dept.	Name & Job Role	Rank / Grade	Date Assured
Procurement	Sheldon Mydat / Karen Hendry	S	12/09/2016
DP	Pete Trainer – DP Service Delivery	SPG3	14/09/2016 & 10/11/16
HR	N/A		
Legal (DLS)	Prit Mandair – Legal		08/09/2016
Property	N/A		
Finance Business Partners	Pat Woodhouse – Finance		12/09/2016 & 10/11/16
Health & Safety	N/A		
DCFD	N/A		

Contents

1	<i>Decisions Required</i>	4
2	<i>Strategic Case</i>	5
3	<i>Economic Case</i>	6
4	<i>Commercial Case</i>	7
5	<i>Financial Case</i>	9
6	<i>Management Case</i>	10

Part 1

1 Decisions Required

This Business Justification concerns the implementation of a security services solution across the Service Integration and Management (SIAM) / Towers model. Currently the MOPAC/MPS have extended a contractual arrangement with Cap Gemini until 31st October 2016 to provide a continuity of services, it is accepted that at current levels this does not provide an adequate and future proofed solution. To move to a SIAM managed solution requires capital investment so that the appropriate tools are in place. This is a foreseen extension to the SIAM /Towers arrangements as articulated in Schedule 2.1 of the SIAM Tower contract.

On the basis that the currently extended legacy arrangement with Cap Gemini, which has a revenue cost of £116,833 per month, expiring 31st October 2016 will ultimately require a further round of tactical negotiations to extend again beyond October 2016; and whilst the alternative solution and proposal from Atos is for a revenue cost of £120,000 per month for a vastly optimised service, the following is thus required:

The Board is requested to note that:

- **£483,000 capital investment from the Service Maintenance Programme (SMP) in the approved DP capital programme in 2016-17 has been made to secure significant time limited discounts (between 45-95%) offered on both the hardware and software elements of the solutions which are achievable due to the relationships maintained by Atos with McAfee and the other suppliers with whom they partnered to deliver security for the Rio and London Olympics and Paralympics; and where the associated volumes of business now make it possible to pass those discount entitlements onto the MPS.**

The Board is requested to approve the following recommendations:

- **£120,000 revenue per month for duration of SIAM contract (48 months from Dec 16) totalling £5.76m. This equates to an increase of £1.4m per annum against an average £9m per annum (including SDIM)**
- **That the costs be funded from savings in the fixed line telecoms contract and application rationalisation and that DP and Commercial manage an action plan to deliver the savings with progress to be reported through Financial Monitoring reports**
- **The extension of the SIAM contract with Atos to an adjusted contract value of £64.19m**

Service	Status	Amount
SIAM (5 year initial term)	Approved	£45.31m
SDIM	Approved	£10.78m
Security Operations Centre (SOC) (Revenue)	Proposed	£5.76m
SOC (Capital)	Approved	483k
SLM	Proposed	£1.86m
Total Contract Value (TCV)		£64.19m

2 Strategic Case

As detailed above the MPS needs to implement a robust and future proofed security solution across the SIAM / Towers model. This solution, delivered by Atos as our SIAM partner, will comprise of four interlocking components;

Protective Monitoring - a critical component of operational security management that provides a mechanism with which to detect Security Incidents. Each Tower Supplier will monitor the Services that they deliver, with the SIAM Supplier consolidating Protective Monitoring logs across the Tower Services. Protective Monitoring provides the largest input to Security Incident Management, a specialised sub-set of Service Incident Management.

Threat and Vulnerability Management - describes proactive activities that aim to reduce the likelihood of Security Incidents across the Tower Services. Threat Management concerns the tactical and strategic activities performed to fuse and analyse intelligence information, from various sources, to improve predication of attacks and shape decision making. Vulnerability Management is about reducing the opportunities of attackers to affect the infrastructure by reducing exploitable flaws in software and hardware.

Security governance – provision of security office integrated with the SIAM.

Forensics support capability – provision of consulting effort to support MPS forensic activities.

In the first instance this will see Atos take over the current service provided by Capgemini, subsequently extending the scope to cover additional zones and provide deeper threat awareness through the introduction of a vulnerability management service. To achieve this MPS needs to make a capital investment in the following;

Product Description	Type	Units	Unit Charge	Total
VnE Manager 4700 Appliance	Hardware	1	£16,721.61	£16,721.61
IP360 Commander	Software	1	£2,531.26	£2,531.26
McAfee Enterprise Security Manager 6000	Software	2	£25,564.86	£51,129.71
McAfee Enterprise Log Manager 5600	Hardware	2	£9,267.19	£18,534.38
McAfee Advanced Correlation Engine 3450	Hardware	2	£10,039.46	£20,078.91
Device Profile Scanner Appliance	Hardware	10	£3,126.52	£31,265.22
McAfee Event Receiver 1260	Hardware	10	£4,053.46	£40,534.56
Intelligence Hub	Hardware	60,000	£0.88	£52,666.67
Target IP Address	Software	60,000	£2.38	£142,666.67
Professional Services	Services	1	£126,123.88	£126,123.88
Total				£483,000.00

3 Economic Case

The purpose of this section is to examine the options for satisfying the business need and recommend a preferred way forward which represents the optimum value-for-money.

In summer 2015 Management Board endorsed the adoption of SIAM and Towers model to manage the MPS IT estate. In late autumn 2015 MOPAC approved the appointment of Atos as the new SIAM partner which effectively brought to an end the relationship and outsourced IT contract with Cap Gemini. We have continued with Cap Gemini on an interim basis for the provision of security services on the understanding that this will not be the end state and because Cap Gemini offered a discounted rate to continue the arrangement. Clearly this is a commercial judgement by Cap Gemini and predicated on them having an opportunity to win the overall contract. It would however be impractical to implement a security solution across the model where Atos were not the security provider as this would lead to undoubted conflicts and would hinder the evolution of the new ways of working.

The original arrangement with Cap Gemini ran at revenue cost of £116,833 per month, the proposal from Atos is for a monthly revenue cost of £120,000 per month with the additional functionality.

To implement the solution Atos need to install various appliances and monitoring equipment across the MPS estate and into Data Centres, the capital investment for that is detailed above i.e. £483,000.

The contract award process allowed for the implementation of a security solution from the successful SIAM bidder subject to commercial review and this process is currently being undertaken in conjunction with procurement and commercial colleagues.

Clearly it is not viable for the MPS to not have a solution in place for IT security management across the estate, especially given the nature of existing and potential future threats. The current interim arrangement with Cap Gemini expires at the end of October 2016, to ensure a solution can be implemented by that date the capital investment has taken place.

4 Commercial Case

The purpose of this section is to outline the proposed procurement approach (or other commercial arrangement) for the achievement of the preferred option identified in the previous section.

As indicated in previous sections the MPS needs to invest in various assets, appliances and hardware to enable Atos to set up and manage the security service effectively across the IT estate. The SIAM Tower contract allows the MPS to purchase the service as detailed under "Optional Services" in annex 1 schedule 2.1 without the need to enter into a tender process but subject to commercial review by MPS stakeholders.

Additional security services were included in the SIAM contract as "Optional Services" which MPS could commission from Atos using the procedure set out in clauses 5.11 - 5.18 of the SIAM Tower Agreement (included below for reference). This contractual hook was included to permit an "award" to Atos without the need for formal procurement process. At the time, all three bidders provided additional security service proposals as part of the procurement activity, thus additional security services were very much within the scope of TTPI procurement.

Relevant section in SIAM Contract:

Optional Services 5.11 & 5.12

As at the Effective Date, the service description for the Optional Services requires further refinement. Following the Effective Date, the Authority intends, but is not obliged, to finalise the service description for the Optional Services. If requested by the Authority, the SIAM Supplier will review and provide feedback to the Authority on any draft services description produced by the Authority.

Following finalisation of the service description, the Authority may require that the SIAM Supplier submits a solution for delivery of the Optional Services together with an outline implementation plan setting out the proposed timescales for implementation of the Optional Services. If the proposed solution and draft implementation plan are acceptable to the Authority it may, at any time, exercise its option to require that the SIAM Supplier provides any or all of the Optional Services by giving written notice to the SIAM Supplier

Atos is ideally positioned to provide the additional security services as they provide service integration across all tower service providers.

The systems and processes that Atos will deploy, are based on those deployed for the Rio Olympics where an unprecedented number of 510 million security events over the period (400 IT security events per second) were successfully managed by the advanced real-time analytics combined with strong security processes to separate genuine threats from digital 'noise' for zero impact on the Games.

Atos is able to offer discounts on both the hardware and software elements of the protective monitoring and vulnerability management solutions. These price discounts range from 40% to 95%. They are achievable due to the relationships maintained by Atos with McAfee and the other suppliers with whom they partnered to deliver security for the Rio and London Olympics and Paralympics; and where the associated volumes of business now make it possible to pass those discount entitlements onto the MPS. These are based on equipment, installation and set-up.

Note: Atos' pricing for Capital (asset) investment, including installation and set-up, consisted of a time-limited pre-Brexit dollar based quotation. This offer was valid for 30 days, which has now expired. Further "post-Brexit" delays have adversely affected Capital cost; the additional cost impact quoted to be a further £90K. Hence in line with local Scheme of Delegation, commitment has been made from Capital budgets for the equipment.

5 Financial Case

The purpose of this section is to set out the implications for the MPS revenue budget and capital plan of the proposed approach.

The cost for security services invoiced by Cap Gemini under the old ICT contract was £116,833 per month. This gave perimeter security and management of user security across the MPS IT estate.

The proposal from Atos is for £120,000 per month for the remaining period of the SIAM contract (48 months from December 2016) which will give an enhanced solution for protective monitoring, security management and governance, management of security across the Towers ecosystem, threat and vulnerability management and the eventual capability for Forensic support services.

The budget implications are:

Capital: The capital investment required enabling Atos to deploy the necessary hardware, appliances and kit is £483,000. The relevant costs for this are broken down in section 2. Provision has been made within the £10m p.a. Service Maintenance Programme (SMP) in the approved DP Capital Plan.

Revenue: The revenue implications of the project are set out in the table below.

Financial year	2016-17	2017-18	2018-19	2019-20	2020-21	Total
Revenue implications (£000)	£480k	£1,440k	£1,440k	£1,440k	£960k	£5,760k
Number of months	4	12	12	12	8	48

The project to define and gain approval for the new ICT security management solution was not completed in time for it to be part of the main contract with the SIAM tower supplier. Provision was not made for revenue costs in the final business case and consequently not in the revenue budget for 2016-17 and onwards.

If the project is approved 2016-17 revenue requirements of £480k will be funded from savings to be made in the fixed line telecoms contract estimated to exceed £1m in that year. Costs from 2017-18 onwards will be funded by a combination of ongoing savings in fixed line telecoms costs and rationalisation of applications resulting in a total estimated saving of £2m per annum. Digital Policing is working with specialist advisors to confirm these savings and this paper recommends a formal action plan around delivery to ensure sufficient savings are achieved.

6 Management Case

The purpose of this section is to explain how the proposals will be implemented and the benefits realised.

Atos will deploy dedicated Security Information and Event Management (SIEM) and Vulnerability Management Security (VMS) infrastructure within the MPS data centres, and will connect remotely over a secured dedicated connection - Atos to MPS WAN circuit to provide Security Operation Centre (SOC) Services, SIEM and VMS platform support. The Atos SOC's located in Moray and Birmingham will have dedicated MPS-specific local network infrastructure deployed from which the SIEM and VMS consoles will be accessed via MPS thin client terminals.

The service will be delivered in three phases:

Phase 1 – to provide The Authority with an Atos Protective Monitoring service to replace the incumbent supplier utilising existing SIEM technology that will be the foundation to cover the entire Tower Supplier environments during subsequent Phase 2 SIEM delivery. This phase will also introduce core vulnerability scanning components to gain visibility of security posture of systems within the Atos Tower environment.

Phase 2 – to extend Protective Monitoring into the wider Tower Provider environments. Additional Event Receiver Collector (ERC) appliances will be deployed into the remaining Tower Provider locations within the MPS Data Centre. Logs from the devices will be on-boarded onto the ERC component. Vulnerability Scanning will be extended into the wider Tower Provider environments. Additional Device Profiler (DP) appliances will be deployed into the remaining Tower Provider locations within the MPS Data Centre. Scan profiles for assets from the devices will be on-boarded into the VMS Manager and regular vulnerability scans scheduled.

Phase 3 – will extend the protective monitoring and vulnerability scanning service to cover wider areas of the MPS estate utilising the core management components deployed in Phase 1.

The SIEM infrastructure will be deployed within the MPS identified data centres. The core SIEM high availability components are presented as physical appliances running deployed into MPS locations. Each SIEM component runs on a hardened Linux operating system which is fully managed, patched and supported by the Atos SOC team.

Key elements:

- Enterprise Security Manager (ESM). This allows access to information from one console providing a central point of administration for system configuration, security policies & settings, reporting and analysis of event and flow data.
- Advanced Correlation Engine (ACE). This provides the SIEM engine with a risk detection engine that generates a risk score using rule-less risk score correlation, and a threat detection engine that detects threats using traditional rule-based event correlation.
- Enterprise Log Managers (ELM). These provide the ability to store raw logs intelligently for compliance, in line with a customer defined retention period. The Log Manager will not alter original log entries or files to ensure compliance with chain of custody.
- Event Receivers (ERC). The ERC's provide the ability to gather and analyse data from event sources including (but not limited to) network infrastructure, security devices, servers, databases, and endpoint protection.

The proposed core VMS infrastructure will be deployed within the MPS Primary data centre. The VMS components consist of a single Scan Manager and distributed Device Profiler appliances. These VMS appliances run hardened Linux operating systems which are fully managed, patched and supported by the Atos SOC team.

Key elements:

- **Vulnerability Manager (VnE).** A dedicated hardened appliance running Linux residing in the MPS Data Centre. The manager appliance allows access to all pertinent information from one console providing a central point of administration for scan configuration, scan scheduling, vulnerability scoring analysis, trending statistics and scan reporting.
- **Security Intelligence Hub (SIH).** Virtual Windows Application and SQL Database Servers residing in the MPS Eagle Data Centre. The SIH component provides custom reporting, dashboards and can store scan data for extended periods of time to perform long-term trend information on vulnerability posture.
- **Device Profilers.** Dedicated hardened appliances running Linux. These devices are the scan engines for the VMS solution. The profilers receive scan tasks from the manager and perform scanning to discover all active IP addresses, identify each host's operating system, applications and vulnerabilities within their associated zone. The device profilers also provide a continuous asset discovery task to identify when new network equipment is connected to the associated network zone.

Atos will provide an Operational Security Director to work in conjunction with the MPS Information Security Officer (ISO) and Tower Security Managers, to ensure the SIAM provides the MPS and the OTS with direction and co-ordination around Information Security that will increase the effectiveness of Information Security across both the Supplier and end user communities.

Consolidated Reports to be provided:

- Security Awareness compliance status for SIAM and other Tower Suppliers
- IAMM (Information Assurance Maturity Model) Status for the SIAM Tower and other Tower Suppliers;
- Compliance to Schedule 2.4 for the SIAM Tower and other Tower Suppliers
- Security Patch Management for the SIAM Tower and other Tower Suppliers
- Security Training Report for all Tower Services
- Report of accounts and permissions information for all End Users for the SIAM Tower and other Tower Suppliers

All required reports will be provided in conjunction with the monthly Service Report or separately upon request