TO:	**CHAIR AND MEMBERS CORPORATE SERVICES COMMITTEE MEETING ON JULY 19, 2016**
FROM:	**MAT DALEY DIRECTOR, INFORMATION TECHNOLOGY SERVICES**
SUBJECT:	**RFP 16-03 SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM REPLACEMENT**

RECOMMENDATIONS

That, on the recommendation of the Director, Information and Technology Services the following actions **BE TAKEN** with respect to the acquisition and implementation of a replacement Security Information and Event Management System:

a) The funding for IBM QRadar Security Information and Event Management System based on the RFP bid price of $157,262.29, HST excluded, (RFP 16-03) **BE APPROVED** as set out in the Source of Financing Report attached hereto as Appendix A;

b) Civic Administration **BE DIRECTED** to proceed with the acquisition and implementation of the IBM QRadar Security Information and Event Management System from the preferred provider, Spyders Inc., in accordance with the Procurement of Goods and Services Policy;

c) Civic Administration **BE AUTHORIZED** to undertake all administrative acts that are necessary in connection with the acquisition and implementation of the IBM QRadar Security Information and Event Management System; and

d) Approval hereby given **BE CONDITIONAL** upon the Corporation entering into a formal contract, service agreement(s) or having a purchase order, or contract record relating to the subject matter of this approval.

PREVIOUS REPORTS PERTINENT TO THIS MATTER

None

BACKGROUND

The City of London uses a Security Information and Event Management (SIEM) system from SolarWinds that is reaching end of life. The system tracks security related information and events in the technology environment. Many of the alerts within the system require research and manual tracking to assess risk which is labour intensive. Alerts include: malware identification, account lockouts, unexpected network behaviour and perimeter security events. Information Security is able to respond to security events, however, the response has been generally reactive. Newer technology allows the events to be correlated in real-time and can show patterns that will allow Information Security to become more proactive in responding to security threats. Implementing a modernized solution is essential to protecting City of London IT assets and data.

Given the ever evolving information security landscape and as our current SIEM is approaching end of life, a Request for Proposal (RFP 16-03) has been completed in accordance with the Procurement of Goods and Services Policy. Six (6) compliant bids were received from proponents and assessed based on established requirements. This assessment included product demonstrations, interviews, presentations, clarification questions and responses. In addition, a technical proof of concept that tested and evaluated the knowledge/expertise of the vendor was successfully completed.

The RFP evaluation team recommended the IBM QRadar SIEM solution to be implemented by Spyders Inc., based on expertise, experience and cost considerations.

DISCUSSION

The acquisition and implementation of a replacement SIEM will support delivery of the identified elements of the *2015 – 2019 Strategic Plan for the City of London:*

Leading in Public Service – 2. Innovative and Supportive Organizational Practices	
What are we doing?	How are we doing it?
C. Enhance corporate and community safety by preparing for and responding to security risks and emergency events.	- Corporate Security Strategic Plan - Emergency Management Strategic Plan - City of London Corporate Emergency Response and Business Continuity Program

IBM QRadar is identified as an industry leader in today's SIEM market and is consistently ranked as a frontrunner in the delivery of these elements. The system will correlate vast quantities of data into what is categorized as violations thereby supplying quality information rather than quantity. This quality information provides a proactive lens into our computing environment allowing Information Security Professionals to address legitimate events as opposed to investigating false positives.

Additional benefits and features of IBM QRadar which support its ranking as an industry leader in the delivery of SIEM solutions include:

- Enhances real time visibility
- Tailors and prioritizes alerts
- Enables more effective threat management
- Produces improved detailed data access and user activity reports

The project will start with a complete and accurate statement of work (SOW). This will set the stage for rollout of the product with precise milestones to track progress and deliver a solution that is tuned to our environment. This project will commence in Q3 2016 and be completed in Q4 2016. Project managers will be assigned from both the City of London and Spyders Inc. with daily status updates to minimize delays and risk to the project. Spyders Inc. past experience with government and specifically municipalities will be leveraged during this project.

Spyders Inc. has successfully implemented the IBM QRadar solution in the following Public Sector environments: University of Saskatchewan, McGill University, The Region of York, and The City of Markham.

Financial Impact

The $157,262.29 in capital funding for the purchase and implementation of the SIEM system is provided for in the approved Information Technology Capital Budget.

The annual licensing, support and maintenance cost of the SIEM system begins at $17,908.37, subject to annual increases, and has been provided for in the approved Information Technology 2016-2019 Operating Budget.

SUBMITTED BY:	**REVIEWED BY:**
EUGENE GRANT, CISSP, HCISPP, CISM, CRISC, CEH **MANAGER, INFORMATION SECURITY**	**TROY THOMPSON, CISSP** **MANAGER, INFRASTRUCTURE AND SECURITY**
REVIEWED AND CONCURRED BY:	**REVIEWED AND RECOMMENDED BY:**
ANNA LISA BARBON, CPA, CGA **DEPUTY TREASURER** **FINANCIAL SERVICES**	**MAT DALEY, MB, BA, MPA, PMP** **DIRECTOR, INFORMATION TECHNOLOGY SERVICES**

c. Dave O’Brien, Division Manager, Corporate Security and Emergency Management
Chris Guinty, CPPB, Procurement Officer