City of
Richmond

August 22, 2011

Business and Financial Services Department
Finance Division
Telephone: 604-276-4218
Fax: 604-276-4162

Attention: To All Proponents

Dear Sir/Madame:

Re: Request for Proposal 4595P Security Information Event Management System - Addendum No. One

This Addendum includes items of clarification, forms part of the Contract Documents and shall be read, interpreted and coordinated with all other parts. Please review and consider the following information in the preparation of your proposal:

1) Please provide a breakdown of the number of servers (Microsoft, Sun, ESX, Red Hat, etc.) that are in-scope.

Physical servers:
Microsoft :30
SUN: 6
ESX: 10
Red Hat: 18

VM servers: (using VM ESX 4.5.)
Microsoft: 50
Red Hat: 5
Oracle: 1
SUN: 1
Linux: 5
CentOS 4/5: 1

It is estimated that the City will expand the number of servers/devices to be monitored by approximately 25% more within the next 5 years

a) If known, what are the expected events per second (EPS) rate for these servers?
We do not have statistics, but for reference, the City currently has 1500+ Active Directory accounts in a Windows 2008 R2 environment

2) Please provide a detailed count of the number of network devices that are in-scope.
Extreme Network Equipment: approximately 30
Juniper Firewall: 1
Iprism: 1

a) If known, what are the expected events per second (EPS) rate for these servers?
We do not have statistics, but for reference, the City currently has 1500+ Active Directory accounts in a Windows 2008 R2 environment

3) Please provide a detailed count of the number of SQL and Oracle databases that are in-scope.
Oracle: 40
MS SQL: 50

a) If known, what are the expected events per second (EPS) rate for these servers?
We do not have statistics, but for reference, the City currently has 1500+ Active Directory accounts in a Windows 2008 R2 environment

4) Please provide a detailed count of the number of applications (NETVault, Exchange, MailChannels, IIS, etc.) that are in-scope
BakBone Netvault backup system (version 8.53) - 1
Exchange 2003 – 6 (to be discontinued by the end of Q1, 2012)
Exchange 2010 – 9 (to be upgraded from existing by Q4, 2011)
Mailchannels application - 1
IIS – approximately 5
Sophos Endpoint Security and Data Protection - 1

a) If known, what are the expected events per second (EPS) rate for these servers?
We do not have statistics, but for reference, the City currently has 1500+ Active Directory accounts in a Windows 2008 R2 environment

5) Are all in-scope devices in a single location or is collection from remote locations required? What is the bandwidth between these locations?
We have two (2) sites, Cityhall and Worksyard, which is approximately 3KM apart in distance. The bandwidth is 10GB using fibre. However, there are plans to relocate our Worksyard in the future; site selection has not been finalized yet but the distance will be within 10-20KM of our Cityhall site

6) What are the requirements for redundancy/high availability/disaster recovery?
There are none for this RFP

7) In regards to Table 2 – Pricing and Warranty Summary, will the City provide details of the architecture, or complete an architectural design document so we can better understand the scope, and size of your environment for pricing? E.G. Number of servers, application, total log volumes, events per second …
See responses to questions 1-4

8) Are there a regulatory (CSOX) or contractual (PCI) compliance mandates that the City of Richmond needs to comply with?
No

9) Can the city provide details on desired log retention requirements (Online, Offline/archive)
Online – real time event analysis and correlation
Offline/archive – ability to review “old” saved events

10) Does the City expect the solution to grow beyond the 265 systems specified? If so, at what rate?
    See responses to questions 1-4

11) Does the City already have a Log Management solution in place?
    We are currently using SPLUNK

12) Are the systems (sources) in scope already configured to generate logs?
    Only for these systems: firewall, URL filter and some Edge switches

13) In items 9 and 10, the City of Richmond indicates general sources it wishes to acquire event log data from. Can this information be expanded to include:
    a) Versions of the sources;
       See responses to questions 1-4

    b) Quantity of each source type; and,
       See responses to questions 1-4

    c) Either expected event rates (per second or per day) or volume of log data generated (per day or week or month)?
       We do not have statistics, but for reference, the City currently has 1500+ Active Directory accounts in a Windows 2008 R2 environment

14) Can the City of Richmond provide any details for event sources that they consider custom? For example, any in-house developed or commercial applications from which they wish to collect event data from.
    Our in-house developed applications use custom Windows server scheduled task event(s)

15) Does the City employ either Microsoft MOM or SCOM for management of Microsoft systems?
    No

16) Section 2.7 - Can the city clarify the intent of requirement**:** *"Able to log security event history"*
    Refers to "Windows events" – ***expected answer is yes or no, provide details of the alternative, if any.***

17) Section 5.1 - Can the city clarify the intent of requirement: *"SSH browsing"*
    Refers to "SSH command line interface (CLI)" – expected answer is yes or no, provide details of the alternative, if any.

18) Section 5.3 - Can the city clarify the intent of requirement: "*JAVA appliance management"*
    Refers to "the web-enabled management interface using JAVA" – expected answer is yes or no, provide details of the alternative, if any.

19) Section 6.3 - Can the city clarify the intent of requirement: *"Able to access different outputs"*
    Refers to the ability to access the SAN using different outputs, which should be detailed by the vendor – expected answer is yes or no, provide details of the alternative, if any.

20) Section 6.7 - Does the requirement refer to output of event data only or storage of event data within the solution?
    Yes to both

21) How many devices are there in total (i.e. in scope for this RFP)firewall, IDP, IDS, URL filter etc.

See responses to questions 1 – 4

22) How many of the 256 physical/virtual servers are Windows, Solaris, VMware, Linux, SQL, Oracle, etc.? Please provide device breakdown.

See responses to questions 1 – 4

23) Please provide model/version of Extreme network devices.

Extreme BlackDiamond 8810, X450, X250, x150 Edge Switches

24) Section 10 - Proposed System Requirements states “other syslog sources”, please provide list of sources

This refers to what other sources your proposed solution is able to report on, which are not already listed in this question

25) Please clarify Table 1, Section 4.5. Is the City looking for the different notification types? Or the different alerts rules? Please explain

As Windows Server 2003 does not have the alerting capability for failed scheduled tasks, we are interested in how your proposed system handles this instance

26) Will you be providing the RFP in Word format? Or the tools to allow the typewriter feature on the PDF?

No

27) Is the City of Richmond open to receiving a proposal whereby a Security Information Event Management System is provided to the City as a Service/Outsource versus having the City run an on-premise solution?

We would prefer to see proposals with an on-premise solution

28) How will the City be providing everyone’s Question and Answer information and is there a time the City expects to get that back to the potential bidders?

An addendum with the City’s responses will be posted to the BC Bid website shortly after the close of accepting questions on August 19, 2011 at 12:00 noon; it will be the bidder’s responsibility to download the files and review the contents

29) Are there multiple geographic sites involved?

Yes, Cityhall and Worksyard locations

30) How many separate networks/address subnets will the SIEM monitor?

See responses to questions 1 – 4

31) How many servers are on the monitored network?

See responses to questions 1 – 4

32) How many users are on the monitored networks?

See responses to questions 1 – 4

33) If taps are being used, will our engineers perform this installation or will those be in place? How many tap points if any?

Taps are not being used

34) What is the total amount of Flows Per Minute (FPS) do you require?

See response to question 33

35) Is Layer 7 flow collection required?

Only if this is a provided feature of your proposed system

36) If port mirroring is used, will our engineers be required to configure them? How many locations require configuration and on what devices?

Port mirroring is not used

37) If utilizing NetFlow, Sflow or J-flow collection, how many devices will be forwarding this traffic? What are the devices?

We are not using these collection types, but we will implement ClearFlow at a later date. See responses to questions 1 – 4 for device types and numbers.

38) Will NetFlow configuration be accomplished by our engineers while on site or will it be in place upon our arrival?

Not applicable

39) The Enterasys SIEM Flow collectors are used to capture raw traffic from the network based on bandwidth via fiber or copper and also 10 gigabit interfaces. What is throughput/bandwidth requirements for collecting raw traffic and will it be fiber, copper or 10 gigabit interfaces?

See response to question 5

40) How many event sources would be sending information to the SIEM?

See responses to questions 1 – 4

41) What is the total amount of Events Per Second (EPS) do you require?

See responses to questions 1 – 4

42) Will Enterasys be responsible for configuring the devices to forward events to the SIEM?

No

43) Is integration with an existing Intrusion Detection System required?

No

44) List all of the devices to be integrated

See responses to questions 1 – 4

45) Will an existing Vulnerability Assessment severs be integrated and if so, what kind?

No

46) Is a SIEM high availability a requirement?

No

Proponents must sign and include this Addendum with their submission.

____

Signature, Name and Title

Yours truly,

Sumita Dosanjh
Buyer II - Contracting Specialist

SD:sd