Port Authority

TO: All Holders of Request for Proposal No. 20-01
Data Center Hosting and Managed Security Services

DATE: March 3, 2020

SUBJECT: Answers to Questions Posed by Interested Parties

The information provided herein below is for informational purposes only. Any changes to the RFP will be by written addendum only and nothing stated in the following material shall be construed as a change or qualification, in any way, to the provisions of the RFP.

QUESTION #1:

Is the Rail Transit Operations (RTO) environment considered the DR environment?

RESPONSE #1: Yes

Yes

QUESTION #2:

Would you consider putting the workloads on the current owned equipment into the total solution?

RESPONSE #2:

Due to time constraints to ensure success for the initial activation, no, but would consider this for a phased future timeframe.

QUESTION #3:

You mentioned that you want the data center/colo to be located within 60 miles. Is that a hard requirement or would you be open to data centers a little further from Pittsburgh?

RESPONSE #3:

Since this is Port Authority owned and managed hardware, we need to be on site ASAP to resolve any service affecting issues. The Port Authority will review options beyond 60 miles, pending ability to gain access as necessary for incident response.

QUESTION #4:

Will Port Authority consider extending the deadline of proposals past the current March 10th deadline?

RESPONSE #4:

Port Authority will extend the period five business days to March 17th.

QUESTION #5:

Are you looking for this to be a Co-Managed solution (i.e. both the customer and service provider have access to the SIEM platform 24/7)?

RESPONSE #5:

Yes

QUESTION #6:

Are there any compliance requirements to be met with this Managed SIEM solution? If so, please describe.

RESPONSE #6:

PCI DSS (SAQ D)

QUESTION #7:

Please describe any recurring operational/security pain points.

RESPONSE #7:

This question is not applicable.

QUESTION #8:

Is there a preference of hosting on premise (physical or virtual), or in the Cloud?

RESPONSE #8:

No preference other than the current physical devices will remain on premise at the co-lo facility.

QUESTION #9:

Is Solar Winds intended to be ingested into the SIEM?

RESPONSE #9:

Port Authority does not do this currently, and this is not a requirement for these services.

QUESTION #10:

What is the breakdown of the listed 222 servers (Windows, Linux, Oracle, SQLserver)?

RESPONSE #10:

The majority are Windows Servers with several Linux servers and appliances. Physical servers are listed in section 4.2.1 of the RFP.

QUESTION #11:

How many Domain controllers?

RESPONSE #11:

3 Domain controllers
2 Read Only controllers

QUESTION #12:

How many users in Active Directory?

RESPONSE #12:

Approximately 1700 various AD objects users – mailboxes etc

QUESTION #13:

Do you currently ingest full netflow data to your current SIEM?

RESPONSE #13:

Yes

QUESTION #14:

What is the average EPS from Palo Alto? Reported from the Palo Interface.

RESPONSE #14:

Logging statistics

Log incoming rate:	245/sec

QUESTION #15:

What are the data retention requirements? (Searchable, Archive)

RESPONSE #15:

We currently retain emails in our Barracuda email archiver indefinitely. As for other data types, there is no current approved data retention policy.

QUESTION #16:

Is it the Port Authority's goal to have the contractor run their vuln detection?

RESPONSE #16:

Vulnerability scanning is listed in the RFP as an optional service. Kindly submit pricing.

QUESTION #17:

Are you looking to augment or replace their existing Qualys scanning or would the Port Authority want the contractor to take over the management of the Qualys environment?

RESPONSE #17:

Vulnerability scanning is listed in the RFP as an optional service. Kindly submit pricing

QUESTION #18:

The current SIEM is Alien Vault and appears to not be in scope for management, but rather the Port Authority is looking to replace with a MSS cloud based SIEM. Is that a correct

interpretation for this RFP?

RESPONSE #18:

Current SIEM is on premises but managed by incumbent vendor. Neutral as to where SIEM resides

QUESTION #19:

On the current SIEM information was provided that the EPS was 120. Can you confirm that is correct EPS?

RESPONSE #19:

Correct as written

QUESTION #20:

Are you requesting Co-Management of devices or just Monitoring?

RESPONSE #20:

Just monitoring

QUESTION #21:

How many total endpoints do you have in place? Servers and Desktops

RESPONSE #21:

222 virtual servers, ~700 virtual desktops and ~130 physical desktops or laptops

QUESTION #22:

How many of those endpoints have Palo Alto Traps deployed on them?

RESPONSE #22:

Roughly 270

QUESTION #23:

Of the total number of servers in scope, how many are critical? IE: DNS, DHCP, Active Directory, Domain Controllers, PII, PCI, etc...

RESPONSE #23:

Port Authority has 3 domain controllers to provide Active Directory Services and DNS. We also operate a set of DHCP servers. A minimum of 38% of the virtual servers run services that require minimal downtime.

QUESTION #24:

Is any cloud infrastructure in scope (AWS or Azure) into the future?

RESPONSE #24:

Port Authority will consider options that meet the stated requirements.

QUESTION #25:

Are you using any Office 365 components?

RESPONSE #25:

Yes

QUESTION #26:

Can you confirm the Next Generation Firewalls Palo Atlo PA3060's OS software version?

RESPONSE #26:

OS version 8.1.12

QUESTION #27:

Please specify if the Next Generation Firewalls Palo Atlo PA3060's Firewall is stand-alone or in an HA Pair?

RESPONSE #27:

PA3060's are HA paired.

QUESTION #28:

Are there any Virtual Contexts on this Firewall? If so how many?

RESPONSE #28:

No Virtual Contexts.

Advanced Endpoint Threat Detection:

QUESTION #29:

How many endpoints are there including servers and desktops? Of those how many do you consider critical?

RESPONSE #29:

See questions #21 and #23

QUESTION #30:

How many high value targets are in the environment? (This would be more associated with people, IE: executives that you would want to have forensics analysis available if a decision is made not to put on all endpoints)

RESPONSE #30:

Port Authority will provide this information to the successful firm upon award.

QUESTION #31:

Can you specify the OS running on the endpoints in scope for the monitoring and scanning of Forensics Analysis if not identified in the RFP?

RESPONSE #31:

Port Authority will provide this information to the successful firm upon award.

QUESTION #32:

Do you have something in place like Snare Enterprise or a centralized Log Management system to convert windows events into syslog? If you don't have this for your windows logs would you like to consider something for Snare Enterprise to accommodate the requirement to convert windows events into syslog? If so, how many licenses will you need?

RESPONSE #32:

AlienVault does this with an included agent. As a bidder, if your solution includes a particular

product, include the pricing for that product as part of your bid. Server count already stated in RFP

QUESTION #33:

What are you using for email? (Office 365 or local exchange server)

RESPONSE #33:

Office 365, though we do have on two on-premises Exchange servers for hybrid mode during the migration.

QUESTION #34:

Is the Barracuda Email Security on-premise or cloud based? If on-premise can you provide Make/Model/Version of the appliance?

RESPONSE #34:

The SPAM filter is a virtual appliance

QUESTION #35:

What are you using for VPN? If you have a concentrator independent of the Firewall please specify what and how many.

RESPONSE #35:

Port Authority uses the Palo Alto firewall for VPN

QUESTION #36:

What are the Operating Systems being used? IE: Windows, Linux, Mac

RESPONSE #36:

A mix of Windows (majority) and some Linux. Mac is not in scope

Log Management/Retention:

QUESTION #37:

Do you have a current log retention policy?

RESPONSE #37:

Yes must be stored for one year with the last three months available in an easily accessible storage (not tape).

QUESTION #38:

Ae you subject to any regulatory or compliance requirements for the retention of raw logs from critical systems? (PCI Suite; SOX/GLBA; HIPAA Suite; FISMA Suite; NERC Suite; ITIL Suite; ISO Suite)

RESPONSE #38:

PCI DSS (SAQ D)

QUESTION #39:

Can you provide the type and quantity of servers that are in-scope for log retention? Example:

Server Types:

Server O/S	Quantity	Core OS Logging	Domain Controller	DNS	DHCP	Web Server	Database
Windows 2008 DC							
Windows 2012 DC							
2008 Web							
2008 DB							
2008 Core							
2012 Web							
2012 DB							
2012 Core							

2003 Web							
2003 DB							
2003 Core							
Windows 2000							

RESPONSE #39:

Specific information about exact OS counts will be supplied to the successful firm upon award.

QUESTION #40:

Can you provide the type and quantity of all other sources, i.e. security devices, which are in-scope for log retention? Example below: IE: Server-Proxy, Server – DNS/DHCP, Server – Active Directory/LDAP, Server- Remote Access, Server – Authentication (RSA/TACACS/Radius), Server – Application(Windows), Server – Application(Unix/AIX/Linux), Server – Web(Windows/Linux/Unix), Server – Mail/SMTP, Server – Database, Server – AS400, Server AV Management Console, Server – End Point Console(IE McAfee, Symantec), Server – Mainframe(# of LPAR's), Infrastructure – Layer 3 switches, Infrastructure – routers, Infrastructure – Wi-Fi Central control(LWAPP), Infrastructure – Wi-Fi(WAP direct), Infrastructure – Load Balancer, Desktop – Windows, Desktop – MAC, Desktop – Linux.

All other sources:

Source Type	Quantity	Internal / External	Description (optional)
Palo Alto NGF, Standalone		external	West Mifflin
Palo Alto NGF, High Availability		Internal	Hosted
Web/Fmail Proxy?			
Juniper SSL VPN	0		
Citrix Netscaler			

Websense	0		

RESPONSE #40:

Specific information about exact device counts will be supplied to the successful firm upon award.

QUESTION #41:

Have you identified a log retention duration (i.e. 1-year raw logs, 90 days index data)?

RESPONSE #41:

One (1) year raw logs retained, with 3 months immediately accessible

QUESTION #42:

What are the number of days needed for indexed data storage (For faster searches)? IE: 30, 60, 90 days

RESPONSE #42:

90

QUESTION #43:

What is the number of months for raw log storage requirements (in compressed format)? IE: 6 months, 12 months

RESPONSE #43:

12

QUESTION #44:

For Windows Event logging do you currently have a collection method in place? I.e. Snare.

RESPONSE #44:

AlienVault Agents collect and forward Windows log events

QUESTION #45:

If no collection techniques are currently deployed for Windows event logging would you prefer an agent based collector for each windows host or a central collector deployed on a physical or virtual Windows server/s?

RESPONSE #45:

We currently use agents from Alienvault.

Vulnerability Management:

QUESTION #46:

How many target IP's are in scope for assessment?

RESPONSE #46:

368

QUESTION #47:

How many are internal IP's?

RESPONSE #47:

336

QUESTION #48:

How many are external IP's?

RESPONSE #48:

32

QUESTION #49:

Is this for PCI?

RESPONSE #49:

Some of our environment is in scope for PCI DSS assessment, the majority is not

QUESTION #50:

Is there a requirement to map to another compliance framework? (IE: HIPAA, ISO, etc...)

RESPONSE #50:

Only currently relevant compliance framework is PCI DSS (SAQ D) for 10 servers

QUESTION #51:

For Internal Assessment, if we use an internal scanner we will need to know how many hosts to assess the number of scanners, but will also need to know what kind of segmentation the client is using to ensure we have an internal scanner placed in the network to allow us to perform the proper testing. Please describe the network segmentation requiring these additional scanners.

RESPONSE #51:

Current Vulnerability scanner is able to scan entire network.

QUESTION #52:

Is the client ok to deploy a virtual scanner for internal IP scanning? (VMWARE would be required to support this option)

RESPONSE #52:

Yes. This is what we currently do

Pen Testing:
Penetration Testing is Goal Based. We don't need to know all the IP's in scope just the target IP's of your critical systems.

QUESTION #53:

How many external target IP's?

RESPONSE #53:

QUESTION #54:

How many internal target IP's?

RESPONSE #54:

12

QUESTION #55:

Can you support VMware for a remote testing appliance related to the internal pen testing?

RESPONSE #55:

We would support a VMWare appliance inside of our network and working logins to our network.

QUESTION #56:

Do you require after-hours testing?

RESPONSE #56:

Yes, after-hours and non-disruptive testing.

QUESTION #57:

Is the pen testing for PCI compliance? If so how many of the target IP's are PCI related? Please specify both internal and external requirements.

RESPONSE #57:

32

QUESTION #58:

Are you requesting quarterly ASV scans for the external IP's that are in scope for PCI?

RESPONSE #58:

Yes.

QUESTION #59:

Would you like to combine the internal and external pen testing with an Endpoint Vulnerability Phishing campaign? A Phishing campaign really tests the users security awareness specific to the targeted systems or IP's associated with the goal of obtaining user credentials or gaining direct system access which then is used in conjunction with the primarily the external portions of the Penetration Test. If this combined test is of interest, please specify how many emails should be included in the campaign specific to the internal and external IP's used in this test.

RESPONSE #59:

Include pricing for this in your proposal if you wish.

QUESTION #60:

We respectfully request and extension of the RFP due date until March 24, 2020. The reason for this additional time is for our team to conduct the necessary due diligence to provide a response.

RESPONSE #60:

See response #4

QUESTION #61:

Page 26 – Can you please confirm that you mean 700 managed end points for the Advanced URL/Web Filtering Section? If so is there a preferred manufacturer or client.

RESPONSE #61:

This refers to a Palo Alto firewall feature.

QUESTION #62:

What is the current version of AlienVault? I.E. Standard, Essentials.

RESPONSE #62:

AlienVault USM Standard

QUESTION #63:

What is the level of data ingestion? 500GB, 1TB

RESPONSE #63:

Information unavailable

QUESTION #64:

We request a two-week extension to allow time to craft our proposal based on the answers to the questions.

RESPONSE #64:

See response #4

QUESTION #65:

Section 2.2.2 requires an agent to be located in Allegheny County. Please define what the County means by agent.

RESPONSE #65:

Per Section 2.2.2 of the RFP an agent is someone authorized to accept notice and service on behalf of the Contractor.

QUESTION #66:

Would the County consider allowing the agent to be located outside of Allegheny County?

RESPONSE #66:

Please submit where your agent is located in your proposal and we will determine if it is sufficient.

QUESTION #67:

Would the Authority be willing to evaluate a hardware solution that would be replacing the current owned solution rather than moving their current hardware?

RESPONSE #67:

See response to #2.

QUESTION #68:

Section 2.3 asks for the Contact name, contract title, address, telephone number and e-mail address of the client's project manager or contracting officer. Is the contact name intended to

be different than the project manager or contracting officer?

RESPONSE #68:

Not necessarily. They may be the same individual providing that person is authorized to bind the contractor in contractual matters.

QUESTION #69:

Section 2.5.4 states copies of the listed certifications should be included in the Appendix, however it is not listed in Section 2.7. Where would the Authority like the certifications to be located within the Appendix?

RESPONSE #69:

They may be placed anywhere within the appendix, but please make sure they are easy to locate.

QUESTION #70:

The RFP requests a statement in the transmittal letter regarding receipt of addendums. Please confirm the term "Transmittal Memorandum" is referred to as the Addendum.

RESPONSE #70:

Please Acknowledge the receipt of all "Transmittal Memorandum".

QUESTION #71:

The Transmittal Memorandum requests signature and return to the address provided. Please confirm this requires a wet-ink signature.

RESPONSE #71:

No, the Transmittal Memorandum do not require a wet-ink signature. They can be submitted electronically to me via email at cterrill@portauthority.org, or mailed to me.

QUESTION #72:

Will the Authority allow Proposers to submit all signed Transmittal Memorandums as part of their response rather than sending in each Transmittal Memorandum upon receipt?

RESPONSE #72:

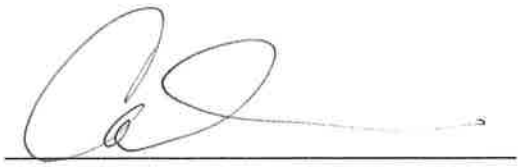
Yes. That would be acceptable.

QUESTION #73:

Would you encourage us to bid on Category #1 if we are NOT ISO9001 compliant?

RESPONSE #73:

If a Proposer has alternate certifications and wants to make a direct comparison, that response will be considered.



Catherine Terrill
Sr. Professional Services Contract Specialist

cc: Project File