PhilaPort
THE PORT OF PHILADELPHIA

Philadelphia Regional Port Authority
3460 North Delaware Ave. 2nd Floor
Philadelphia, PA 19134

November 14, 2022

To: All Bidders

From: Kate Bailey
Director of Procurement

Re: ADDENDUM NO. 4
22-083.S – RFP for PAMT Cyber Security Assessment and Training Program

This Addendum No. 4 is issued to:

1. Extend the Proposal Submission Deadline from **Tuesday, September 13, 2022, at 2:00 PM until Wednesday, November 23, 2022, at 2:00 PM.**

2. Provide responses to the following questions:

Q1: We received this RFP and although we don't conduct risk assessments, or penetration testing, we do offer cyber security awareness training. Will that also be part of your Cyber Security Awareness initiative and if so, will you be sending an RFP specifically for that?

A1: Training services will be made part of the contract for this project.

Q2: Does PAMT require interviews and documentation review to be conducted onsite?

A2: No. This can be done remotely.

Q3: Can PAMT Provide the following for both internal and external penetration scope:

a. Number of external IP addresses in scope ?

b. **Number of external applications addresses in scope ?**

A3: a. Number of external IP addresses in scope ? three (3)

b. Number of external applications addresses in scope ? three (3)

Q4: Are there any time-of-day restrictions in which the internal and external penetration testing can be performed ?

A4: Successful vendor will need to coordinate with tenant. Testing may not be performed during terminal operations and will be outside of normal business hours.

Q5: Will PAMT provide account credentials as part of the internal and external penetration testing ?

A5: No.

Q6: Since this is not a contract for construction, will PAMT waive the requirement that we be required to participate in the Apprenticeship Program ?

A6: Requirement waived.

Q7: What is the "Vendor Data Management Unit Number ?

A7: For Proposals to be considered for award Offerors must obtain a Vendor Management Unit Number. To register for the Vendor Management Unit Number visit www.vendorregistration.state.pa.us or call 717-346-2676.

Q8: Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?

A8: PhilaPort has never contracted for these services for PAMT before.

Q9: Specify the VLAN details how many are included in the Scope?

A9: 7 at PAMT.

Q10: Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.?

A10: 18 physical, 400 Network Devices.

Q11: How much (%) of the infrastructure is in the cloud?

A11: 10%

Q12: In the IT department/environment, how many employees work?

A12: 10.

Q13: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

A13: Yes, we manage our own data center.

Q14: Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

A14: PhilaPort does not disclose budgetary information.

Q15: Would you kindly allow us to write on more pages (20 pages) since the 10-page limit is too short?

A15: The page limit will be raised to 15 pages.

Q16: Is there a specific count to internal and external IP addresses?

A16: Approximately 2000.

Q17: Is there an asset count? (pc's, servers, wireless access points, printers. etc.)

A17: 18 servers, 700 devices.

Q18: What is the employee count for PAMT?

A18: 400.

Q19: Does the penetration testers have to be onsite for the testing?

A19: No.

Q20: Is there a specific timeline for the risk assessment to be completed?

A20: No. Offeror to provided schedule per the RFP documents.

Q21: Are the cranes manned or unmanned?

A19: No.

Q22: Are there any policies that need to be reviewed in this assessment?

A22: Yes.

Q23: Will the OT & IT devices need to be assessed?

A23: No.

Q24: Are there any SCADA systems?

A24: No.

Q25: Is it necessary that proposals be submitted via the portal and in hard copy, or is submitting via the portal sufficient?

A25: Offerors must follow direction in RFP Section III, D – Submission of Proposals. In addition to instructions on submitting via the portal, Offerors must also follow directions on submitting original signature forms:

> Within one (1) business day of the proposal submission date, the original Form for Submission of Proposal (Appendix A) shall be delivered to:
>
> Kate Bailey
> PhilaPort
> 3460 North Delaware Avenue
> 2nd Floor Philadelphia, PA 19134

Q26: Can the Port share its budget for this project?

A26: See A14.

Q27: How many IT employees does the Port have? Is IT centralized?

A27: 10, yes.

Q28: For internal penetration testing, are there any IPs are in scope? If so, how many?

A28: Need more information.

Q29: How many physical locations are in scope for internal penetration testing?

A29: 1.

Q30: For external penetration testing, how many IPs are in scope?

A30: 3.

Security Assessment

Q31: Page 5 of 65 mentions a training program. Is there more information on what type of training program is requested from the port of Philly?

A31: Cyber Awareness.

Q32: How big is the environment that the security assessment and Penetration Testing will be performed?

A32: Question too vague to respond.

Q33: Is there a desired timeline when Assessment and Penetration Testing would like to be completed by?

A33: See A20.

Q34: How many internet facing hosts are there?

A34: 3.

Q35: Is there a preference on a framework that the Port of Philly would like to be assessed against?

A35: No.

Q36: How many hosts are in scope for penetration testing?

A36: 3.

Q37: What Operating Systems will be assessed/pen tested?

A37: Windows, Unix, IBM i.

Q38: Will Servers be in scope?

A38: No.

Q39: Will we be allowed to install tools or agents?

A39. No.

Q40: Will the writing of policies or procedures be required?

A40: No.

Q41: Are offshore resources allowed to work on this project?

A41: No.

Q42: Are references required?

A42: Yes. References must be included per the instructions in the RFP Document.

Physical Security Assessment

Q44: On Page 3, the RFP states that Port of Philadelphia is looking for "Physical intrusion attempts into one or more target locations." At minimum, how many locations does Port of Philadelphia envision to be in scope?

A44: 1.

Q45: Are there any restrictions or limitations into methods of intrusion?

A45: Yes, cannot affect terminal operations.

Q46: During the physical intrusion phase, will there be a Port of Philadelphia employee escort provided in close proximity to the Contractor?

A46: Will discuss with successful Offeror.

Q47: For legal and liability reasons, please detail what kind of force (lethal or non-lethal force) a Contractor should expect from the physical intrusion. If there is lethal or non-lethal force, please share how Port of Philadelphia will manage the life safety of the Contractor's employees conducting the physical intrusion.

A47: Facility is manned by security personnel 24/7. For unescorted access to the facility, personnel will be required to have a valid TWIC. For escorted access, personnel will be required to have a valid phot identification and will be subject to an escort fee.

Q48: Is the physical intrusion expected to be conducted during business hours or outside of normal business hours?

A48: See A4.

External Penetration Test

Q49: We understand contractor is responsible for conducting their own intelligence. To that end, for pricing, timeline, and resourcing purposes, please share how many external IP addresses are likely to be in scope.

A49: 3.

Q50: For social engineering/phishing emails, will Port of Philadelphia be providing additional email addresses beyond ones discovered by the Contractor? If yes, approximately how many social engineering/phishing emails is Port of Philadelphia expecting to be sent?

A50: Will be discussed with successful Offeror.

Q51: What type of external penetration test is Port of Philadelphia expecting to be performed? (Black box, white box, gray box, etc.)

A51: Black box.

Q52: Is the external penetration test expected to be conducted outside of business hours?

A52: Yes.

Internal Penetration Test

Q53: For our scoping purposes, when was the last date the Port of Philadelphia updated their IT asset inventory lists?

A53: September 2022.

Q54: What type of internal penetration test is Port of Philadelphia expecting to be performed? (Black box, white box, gray box, etc.) - REPEAT OF Q51

A54: Black box.

Q55: Is the external penetration test expected to be conducted outside of business hours.

A55: See A52.

Q56: On page 3, it states that "Remote use of network-based vulnerability scanners to identify live hosts and assess in-scope Internet accessible systems and network devices". Is our understanding correct that the internal penetration test is to be conducted remotely?

A56: Yes.

Q57: For pricing, timeline and resourcing purposes, please share how many internal IP addresses are likely to be in scope.

A57: 250.

Q58: Beyond the corporate offices, are there any other shared facilities with Shipping Companies or Public Safety Answering Points (PSAPs) that may be in scope as part of this engagement?

A58: No.

Misc. Questions

Q59: Is there currently an incumbent on an existing contract or similar contract? If yes, who are they (individual/firm name), the value of the contract and are they eligible to bid on the contract? Is the incumbent performing to the satisfaction of the contract manager and/or Port of Philadelphia?

A59: See A8.

Q60: What is the estimated budget Port of Philadelphia has set aside in anticipation of awarding this contract?

A60: See A14.

Q61: What is the expected timeline of when this project is to begin and expected to be completed?

A61: See A20.

Q62: Is this penetration test being used as part of any annual audit, risk management, regulatory or compliance programs? If yes, which ones?

A62: No.

External Infrastructure

Q63: Total number of live/active Internet facing IP addresses

A63: 3.

Q64: Types of publicly accessible services (e.g. FTP, SFTP, SMTP)

A64: FTP, SFTP, SMTP.

Internal Infrastructure

Q65: Number of workstations?

A65: 150.

Q66: Number of servers?

A66: 18.

Q67: Which operating systems are in use?

A67: Windows, Unix, IBM i.

Q68: Is the network segmented or flat?

a. Can all networks/VLANs in scope be accessed from one network point?

b. Number of networks/VLANs in scope?

A68: a. Can all networks/VLANs in scope be accessed from one network point? Yes.

b. Number of networks/VLANs in scope? 7.

Q69: Is there any Wireless capability?

a. Is the solution centrally configured?

b. Number of Access Points?

c. Number of SSIDs broadcasted?

d. Are 2.4Ghz, 5Ghz, or both frequencies broadcasted?

e. What types of authentications are in use, if any?

A69: Is there any Wireless capability? Yes

a. Is the solution centrally configured? Yes

b. Number of Access Points? 30.

c. Number of SSIDs broadcasted? 5.

d. Are 2.4Ghz, 5Ghz, or both frequencies broadcasted? Both.

e. What types of authentications are in use, if any? Wep, wpa2, AES.

Q70: Where is geographical location of the internal environment?

a. If there are multiple sites, where are the locations for each?

b. Can all locations be accessed from one main site?

A70: Packer Ave Marine Terminal in Philadelphia, PA.

a. If there are multiple sites, where are the locations for each? No.
b. Can all locations be accessed from one main site? Yes.

Remote SE

Q71: Number of Staff?

A71: 50.

Q72: Details of any corporate remote access systems e.g. Outlook Web Access, SSL VPN etc.

A72: VPN, gotomypc.

Q73: What is the desired outcome of the engagement? Click counting, credential harvesting, compromise workstation and gain a foothold onto the network?

A73: To identify our weakest links and address them accordingly.

Q74: What are your primary security concerns?

A74: Phishing, ransomware.

Q75: Are there any particular targets that you would like to put forward, or should this be an untargeted attack based on our own reconnaissance?

A75: Untargeted.

Physical SE

*** need to coordinate with terminal security for this section ***

Q76: What are the principle security concerns? What are they looking to test in this physical security assessment (people, physical security systems)?

A76: Access control procedures and access to CCTV and access control systems.

Q77: What are you looking to test in this physical security assessment (people, physical security systems)?

A77: People and systems.

Q78: Is there any specific technology in use we should know of ahead of time (video cameras, alarm systems, etc)?

A78: CCTV system (American Dynamics).

Q79: How large is/are the in-scope client site(s)? (Square footage)

A79: 100 acres.

Q80: How many employees typically work in the in-scope office(s)?

A80: Number varies.

Q81: How many sites are in scope and what are the addresses?

A81: One Site located at 3301 South Columbus Blvd, Philadelphia PA.

Q82: Are the in-scope locations within a shared office environment?

A82: Yes.

Q83: If so, is the office on multiple floors or just one?

A83: One floor.

Q84: Which testing approach is the customer interested in? (We generally recommend phase 2)

a. Phase 1 - Enumeration / Reconnaissance – consultant performs enumeration and reconnaissance on the organizations external building and office infrastructure and employees, to identify any information that could help shape or define the attack delivery phase.

b. Phase 2 - Technical Review – consultant, either escorted or alone depending on the engagement type, reviews the physical access controls outside and inside the client building / office

c. Phase 3 - Attack Delivery – information gathered in phase 1 and/or phase 2, define the technical approach. The building and employees are targeted, and the tester attempts to drop an initial foothold network device or access the sensitive information, room, hardware as told by the client.

d. **Phase 4 – Post-Exploitation – assuming the attack delivery phase is successful, the consultant will then attempt to leverage the initial compromise by obtaining data from the compromised system and potentially enumerating areas of the internal network. Additionally, consultants will attempt to maintain persistence to any compromised hosts.**

A84: Phase 2.

Q85: Has the customer engaged in previous physical security or physical social engineering testing previously, and if so, what were the results?

A85: Yes. Cannot provide information publicly for security purposes.

Q86: How many devices, users, and servers will be required to scan?

A86: See Q17 for devices and servers.

Q87: What is the operational system environment?

A87: Secure client-controlled room.

Q88: Are there any high value assets?

A88: Yes.

Q89: What existing Service Level Agreement (SLAs) are in place?

A89: Cannot provide information publicly for security purposes.

Q90: Are there any homegrown applications that need specialized attention?

A90: No.

Q91: Do they have an existing secondary data center? Cloud or Local.

A91: Yes. Off-site.

Q92: Please state the specific compliance type you are aiming to accomplish?

A92: Internal

Q93: Is PhilaPort looking for animated-character scenario-based training?

A93: This is not a training requirement.

Q94: Does the contractor need to have an off-site web-based training portal or will the training modules be integrated in an government-owned Learning Management System or learning platform?

A94: Will not be integrated in a government-owned Learning Management System or platform.

Q95: How many users will need to be trained?

A95: 100.

Q96: Is PhilaPort looking for live-actor interactive simulation training for clear understanding of risks and vulnerabilities?

A96: This is not a training requirement.

Q97: Will the training be focused on teaching Cyber and IT personnel how to conduct risk assessments and penetration testing?

A97: Cyber

Penetration Testing:

Q98: Can the customer provide an estimate on how many assets (Hosts, IPs, Internal/External Applications, etc.) will be in-scope for the penetration test?

A98: 250

Q99: Schedule: *"PhilaPort has established the weight for the Cost criterion for this RFP as 10% of the total points. The schedule criterion is rated by giving the proposal with the shortest schedule the maximum number of cost points available."*

- **Does the customer have any sort of required date of completion for this project? For example, will all deliverables need to be submitted by the end of 2022.**

A99: See A20.

Q100: *"The Technical Proposal is limited to ten (10) pages. This excludes information on key personnel."*

- **Does the customer have any requirements for the key personnel? Number of key positions, minimum years of experience, required certifications, etc.?**

A100: Offerors should provide any information/background on key-personal that is applicable or relevant to this project.

Q101: **Submission:** **Is there a font size and type requirement for the proposal?**

A101: Font type shall be Times New Roman and must be no smaller than 11 pt.

Q102: *"Within one (1) business day of the proposal submission date, the original Form for Submission of Proposal (Appendix A) shall be delivered to:"*

- **To clarify, Parts I, II, and III of the proposal are to be submitted through Bonfire and then the original Appendix A should be mailed to the given address?**

A102: That is correct. See A25.

Q103: *"If applicable, Offeror's team will have sufficient personnel that possess Transportation Worker Identification Credentials to gain access and properly perform the Services."*

- **Is this applicable?**

A103: This requirement has been deleted. Any access to the site will be arranged through the tenant.

Q104: *"Contractor agrees that each of the Identified Contractors will be paid at least five (5) percent of the Proposal Amount and that the combined total amount paid to the Identified Contractors shall be at least twenty (20) percent of the Proposal Amount"*

- **Are the identified contractors, contractors we have identified or is there a list that PhilaPort will provide?**

A104: Section XXI. Diversity and Inclusion of the General Conditions of the RFP document (Page 44 of 65 of the RFP .PDF File) is not applicable to this project.

Q105: *40 CFR Part 33 Subpart C (page 61 of RFP)*

- **For such a small project, we do not plan to subcontract any of this work out, is this still applicable for us?**

A105: All Offerors are subject to 40 CFR Part 33 Subpart C. Please note, this subpart does not require subcontracting with a DBE.

Q106: Does PAMT currently use any SaaS cloud-based software?

A106: Yes.

Q107: Does PAMT currently use any cloud-based data storage?

A107: Yes.

Q108: Does PAMT expect Penetration Testing to include external cloud-based systems (either software or data storage)?

A108: No.

Q109: Will the engagement be limited to reviewing the cyber security practices of the Packer Avenue Marine Terminal (PAMT), or will it include other terminals / locations managed by PhilaPort?

A109: Although the tenant has other facilities in the area, the scope of work for this project only includes the Packer Avenue Marine Terminal.

Q110: Does PhilaPort wish to include assessment of OT / IoT cyber security practices in this effort, or strictly IT security?

A110: strictly IT security

Q111: Does PhilaPort have a preference in standards used to conduct the assessment portion of the engagement (i.e. ISO27001, ISA/IEC 62443 for OT/IoT, NIST CSF, leading practices, etc.)?

A111: No preference

Q112: While conducting external penetration testing, will the scope be limited to systems physically located within the PAMT facility, or will all PhilaPort internet-facing systems be considered in scope?

A112: Yes.

Q113: Does PhilaPort know the size / amount of internet-facing IP address ranges to be considered in scope for external penetration testing? (e.g. two /24s; or one /16)

A113: 3 /24.

Bidders shall acknowledge receipt of this addendum by immediately emailing a copy of the completed acknowledgment to Kate Bailey at procurement@philaport.com

---

ACKNOWLEDGMENT OF RECEIPT OF ADDENDUM NO. 4
Project #22-083.S
RFP for PAMT Cyber Security Assessment and Training Program

Date__________

By________________________________

Company___________________________

Telephone__________________________

Fax_________________________________

Email _______________________________