PORT OF OAKLAND

Purchasing Department
530 Water Street
Oakland, CA 94607

Date: **October 7, 2022**

ADDENDUM No. 1

RFP No. 22-23/08 – Cybersecurity Vulnerability Assessment

This Addendum modifies the original RFP Documents for the above-mentioned RFP. **Acknowledge receipt of this addendum in the space provided on the RFP Acknowledgement and Signature Form (Attachment 3). Failure to do so may disqualify your proposal.**

The following questions were submitted by the deadline and are answered in this addendum:

General Questions

1. **Supplier Question**: Can the Port grant an extension on the due date?

   ***Port Response**: No*

2. **Supplier Question**: Will there be a stakeholder meeting for the review of the vulnerabilities found? If so, is this meeting to held in person?

   ***Port Response**: The required deliverable is a report with findings and data as per Section II, Scope of Services, Items C and D. No in-person meetings are required to present the findings. The Proposer may choose to walk through the findings with the Port Project Manager and Project Team, which may be held via Zoom or other online meeting tool.*

3. **Supplier Question**: Will the scope of the penetration testing be clearly defined and signed off by senior management?

   ***Port Response**: The scope of the Penetration Testing will be reviewed and approved by the Port.*

4. **Supplier Question**: What is the skill level of the staff that will remediate the findings?

   ***Port Response**: Remediation of the findings and related questions is outside the scope of this engagement. The Port will determine whether, how and by whom, the findings will be addressed.*

5. **Supplier Question**: How many Port staff work in the IT Department/Environment?

   Port Response: *This question is not relevant to the desired scope.*

6. **Supplier Question**: Will the written policies and procedures be required to be updated in this assessment?

   Port Response*: No.*

7. **Supplier Question**: How often is the assessment expected to occur? Monthly? Quarterly? Annually? Will continuous monthly vulnerability scanning to maintain the networks resiliency?

   Port Response*: The scope requires annual vulnerability scanning.*

8. **Supplier Question:** Is this considered a full-time effort at 40 hours per week per person on staff or an effort that just happens at a certain time once a year?

   Port Response: *The scope requires annual vulnerability assessments. The Port will provide the necessary resources to support the engagement and facilitate access.*

9. **Supplier Question**: Is there a time frame when the penetration testing can be conducted? Considering adversaries could attempt any time of day.

   Port Response: *The testing can be done at any time for most systems. The Port will coordinate on sensitive systems for desired times in case there is unanticipated impact.*

10. **Supplier Question**: How many workstations (stationary and mobile) does the Port have?

    Port Response: *Please refer to the Environment description under Section II, Scope of Services.*

11. **Supplier Question:** What SaaS services does the Port use?

    Port Response: *Details on the applications will be provided once a mutual interest has been established.*

12. **Supplier Question**: Is the Port exempt from local, city, county, or state taxes?

    Port Response: *No.*

13. **Supplier Question**: How many end-users does the Port have?

    Port Response: *Assume approximately 500 end users for testing.*

14. **Supplier Question**: What is the Port's goal(s) of an attacker you want a firm to simulate?

    Port Response: *The Port is open to various solutions. Please describe your approach in your Plan and Approach.*

15. **Supplier Question**: Will testers be granted any level of initial access prior to the start of the penetration test (e.g., standard user credentials to simulate insider threat)?

    Port Response: *Please describe your Plan and Approach. If such accounts or access are required, those can be provided.*

16. **Supplier Question**: Will testers need to provide Personally Identifiable Information (PII) for testing?

    Port Response: *On-site testers will be required to provide PII to access Port facilities.*

17. **Supplier Question**: Will the assessments/testing be performed onsite or remotely? Can PenTesters perform all work virtually? Can team members work from an offshore location?

    Port Response: *Please describe your approach in your response. While the Port would prefer an on-site assessment, the Port can accommodate onsite, remote, or a hybrid.*

18. **Supplier Question**: Please provide the number of physical locations does the Port have? If there is more than one Physical Location, are these locations networks connected?

    Port Response*: The three (3) primary business locations described in the beginning of Section II. Scope of Services are in scope for the wireless penetration test.*

19. **Supplier Question:** Is the Physical Security run by you or the building managers at these location(s)?

    Port Response: *Physical security is outside the scope of this effort. The Port will facilitate any on-site access to necessary Port facilities that the Proposer may need.*

20. **Supplier Question:** Is there a Cyber Annex in place for the United States Coast Guard for the Port? What compliances does the Port authority have to meet the requirements? (i.e. United States Coast Guard, FAA, TSA, etc.)?

    Port Response: *The Port has a U.S. Coast Guard approved Cyber Annex within our Facility Security Plan. The Port meets all USCG/Federal requirements and is subject to annual audits by the local Captain of the Port as well as random/frequent unannounced inspections.*

21. **Supplier Question:** Does the Port have a zero-trust communication system in place for the reports and data to be sent securely to the Port authority? Is there a specific format that the data and reports should be sent in?

    Port Response: *There is no specific format for the report. The Port can provide a secure method for upload of the reports, data, or any other communication if needed by the Proposer.*

22. **Supplier Question**: Are there network perimeter defense technologies current used across the system? (i.e., Firewalls, Load Balancers, IPS/IDS, etc.)

    Port Response: *Yes.*

23. **Supplier Question:** Can all production networks be accessed from a single location for testing purposes?

    Port Response: *Assume having to visit two (2) locations for testing purposes.*

24. **Supplier Question**: How many technical documents does the Port have (network, diagrams, visio dosc, process documents, etc.), and how many Information Security documents do you have (AUP, NDA, InfoSec Policy, etc), what is the total estimated quantity of pages, and can these documents be made available during the engagement?

    Port Response: *Necessary documentation can be provided during the engagement. Assume about 100 pages.*

25. **Supplier Question:** Is this testing engagement required to fulfil any specific regulatory/compliance needs and if so, which frameworks?

    Port Response: *The testing is to be provided to the Port. The Port may use the results as it sees fit.*

26. **Supplier Question:** Are there any systems that would be tested which could be characterized as fragile (systems with tendency to crash)?

    Port Response: *We will provide those details prior to any testing and will coordinate timing as appropriate.*

27. **Supplier Question:** Are there any systems on the network which the client does not own, that may require additional approval to test?

    Port Response: *In general, no. The Port will coordinate any necessary approvals.*

28. **Supplier Question:** Are there any 3rd parties that need to be notified of the testing activities? (Ex: 3rd party hosting platform that hosts the website which the customer owns and wants tested.)

    Port Response: *The Port will coordinate any approvals for such items.*

29. **Supplier Question:** Is management aware that a test is about to be performed?

    Port Response: *Relevant management will be informed prior to testing, and the firm conducting the tests will have all necessary approvals from the Port before testing begins.*

30. **Supplier Question:** Regarding your four locations (two in the airport, the office building, and harbor facilities) can their LANs all be reached via private connections (ex vpns, mpls, etc)?

    Port Response: *Yes, however assume having to visit two (2) locations for testing, as it is not advisable to be testing over WAN links.*

31. **Supplier Question:** Regarding External Testing, how many DNS domains are included? (Ex: vpn.portofoakland.com and rdp.portofoakland.com are the same domain)

Port Response: *Assume about 10.*

32. **Supplier Question:** Regarding "II.A.3: Virtual Infrastructure Assessment", is this referring to VM's hosted in your datacenters/server farms or VMs hosted in a cloud environment (ex AWS/Azure/GCP/etc)

    Port Response: *On-premise VM environment*

33. **Supplier Question:** How many users/employees do you have?

    Port Response: *Assume under 1,000 user accounts.*

34. **Supplier Question:** How many distinct environments should be evaluated? (ex on-prem, could, unique business/operations silos)

    Port Response: *Assume about 10 distinct environments.*

35. **Supplier Question:** What network perimeter defense technologies (their vendors and quantity of devices) are currently used across the system ? (ex: Firewalls, Load Balancers, IPS/IDS, etc)

    Port Response: *Defense technologies are considered sensitive information and cannot be disclosed publicly. Once a mutual interest has been established, additional details can be provided. For the purposes of responding, assume that defenses are in place using mainstream technologies.*

36. **Supplier Question:** Is your IT infrastructure fully self-managed?

    Port Response: *Yes*

37. **Supplier Question:** If you use a MSP/MSSP to assist with managing your IT infrastructure, what is the company and what components do they manage on your behalf?

    Port Response: *N/A*

38. **Supplier Question:** Regarding section "II.A.7. Network Configuration Review (including LAN, DMZ, Firewalls, and Routers)", please confirm the quantity of ACL's and/or Firewall Policies configured on these devices.

    Port Response: *Approximately 650.*

39. **Supplier Question:** Regarding section "II.A.7. Network Configuration Review (including LAN, DMZ, Firewalls, and Routers)", are any of your firewalls performing deep packet inspection (full packet decryption)?

    Port Response: *Yes*

40. **Supplier Question:** Regarding section "II.A.9. Review of Patch management Practices for Network Devices, Servers, and Endpoints", are you using a vulnerability scanner internally, if so who is the manufacturer?

    Port Response: *The Port's other vulnerability assessment tools are outside the scope of this engagement. The Proposer is expected to assess the Port's Environment with their own tools.*

41. **Supplier Question:** Regarding section "II.A.9. Review of Patch management Practices for Network Devices, Servers, and Endpoints", Does this include IoT/OT devices? If so, how many?

    Port Response: *OT devices are segmented and are out of scope.*

42. **Supplier Question:** Regarding items II.A.7. through II.A.11. would you find a policy review acceptable or is a manual review of configurations required?

    Port Response: *An actual review of in-place systems is requested.*

43. **Supplier Question:** Does Port of Oakland use AWS?

    Port Response: *No*

44. **Supplier Question:** Does Port of Oakland use Azure?

    Port Response: *Yes*

45. **Supplier Questions:**
    - If Port of Oakland uses Azure: please describe the cloud strategy/purpose for this enviorment.
    - If Port of Oakland uses Azure: Please identify if this is a production, development, and/or UAT environment
    - If Port of Oakland uses Azure: Can a network schema or logical diagram be made available during the engagement?
    - If Port of Oakland uses Azure: How many regions are you deployed in?
    - If Port of Oakland uses Azure: How many tenants do you have?
    - If Port of Oakland uses Azure: How many application services are used?
    - If Port of Oakland uses Azure: Which services are used (Ex: Compute, Networking, Firewalls, DNS, Identity, Azure Functions, Azure Kubernetes Service, Storage, etc)

    Port Response: *This is a production environment; Network diagrams can be made available during the engagement; we are in two 2 regions with 1 tenant with Compute, Networking, Load Balancer, Firewalls, Identity, Storage, and Azure functions in place.*

46. **Supplier Question:** Does Port of Oakland use GCP?

    Port Response: *No*

47. **Supplier Question:** Does Port of Oakland use other cloud providers (OVH, RackSpace, etc)?

    Port Response: *No*

48. **Supplier Question:** As you are aware, we are entering a highly inflationary period. Would the Port be willing to look at a pricing model that factors in benchmarked inflation rates to calculate adjustments over the contract, or do you expect us to make those estimates ourselves and adjust our pricing today to provide a fixed price? Please advise.?

    Port Response: *As per Section II, Scope of Services, Item F, a fixed fee is expected for these services.*

49. **Supplier Question**: The RFP requests fixed 5-year pricing with the option to extend to 7 years in Section II G., Projected Time Line and Contract Length. In the security space, risks and compensating tools and techniques change regularly. Does the port expect a quote based on existing tools and strategies with the understanding that there may be additional tools and strategies over the course of the contract? We will then make recommendations based on threats and our experience within the port environment. Any additional items would be provided with similar discounts as the existing contract.?

    Port Response: *Please describe your approach in your Plan and Approach. As a fixed fee is required, a Proposer should plan to adapt their approach over time to remain relevant over the course of the Contract. A Proposer that chooses to use a known outdated approach in later years of the contract would likely be viewed upon negatively by the Selection Committee.*

50. **Supplier Question**: 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?

    Port Response: *This question is not relevant to the Request for Proposal. Suppliers are requested to respond based on the information contained within the RFP and any addenda, not past practice which may not be relevant.*

51. **Supplier Question**: How many FTEs (Full Time Employees) were on the previous contract? Has the PWS (Personal Work-Stations?) changed? What are your KPIs (Key Performance Indicators)?

    Port Response: *This question is not relevant to the Request for Proposal. Suppliers are requested to respond based on the information contained within the RFP and any addenda, not past practice which may not be relevant.*

52. **Supplier Question**: If a company has a teaming agreement with a subcontractor, does the subcontractor's experience count as experience for the prime?

    Port Response: *The proposed team will be evaluated based on the Evaluation Criteria in Section V. The subcontractors will be considered as part of the team.*

53. **Supplier Question**: Is there an intended financial budget range amount for this project?

    Port Response: *No, but costs are weighted according to Section V. Evaluation Criteria.*

54. **Supplier Question** Can proposers use digital signatures to sign documentation that will be submitted in their proposals or do all signatures need to be wet signatures?

Port Response: *Proposal documents that indicate a signature is needed can be scanned and uploaded to Liquid Files, either the original hard copy or one that has been digitally signed. All submissions must meet Section IV Submission Requirements, Submittal Format, see page 4 & 5 of 10.*

55. **Supplier Question**: The RFP delineates a 32-page limit but then defines it as a 16-page limit for double-sided page responses. Since submissions will be digital PDFs via the Port's portal, the pages will not be double-sided double sided. Please confirm that a 32-page single-sided response is acceptable?

Port Response: *Per RFP Section IV. Submission Requirements, Submittal Format, page 10, states response may not be longer than 32 pages in total.*

56. **Supplier Question**: Please confirm if it is acceptable to use an appendix in order to include all required forms such that they will not count toward the page limit, as per RFP Section IV: Please limit your total response to the number of pages indicated below. (Excludes the required attachment forms provided with this RFP)?

Port Response: *The appendices count towards the page limit.*

57. **Supplier Question**: Is there any chance a firm could provide some of the services? Or the only way to participate is by accepting all the services?

Port Response: *The Port is looking for a firm that can provide all the services as outlined in the RFP Scope of Services.*

External Network Questions

58. **Supplier Question**: How many Internet Endpoints does the Port have? Does the Port share any of these endpoints or any networks with another company? Are any of the endpoints detailed in RFP, what is exposed to the internet and represents the scope for External Penetration Testing (e.g., web servers, VPN endpoints, APIs)?

Port Response: *Please refer to Section II. Scope of Services, first paragraph. In additional items such as switches, IP cameras, etc., were not included in the breakdown. All endpoints are located in facilities owned by the Port: the Oakland seaport, Oakland International Airport (OAK), and the Port's commercial real estate division.*

59. **Supplier Question**: Can the Port provide the approximate number of **live external IP** and **live internal IP** addresses in scope for the external network penetration test? Of the 5000 endpoint devices, approximately 2050 of them are detailed as servers, workstations, WAPs, and IP phones. What are the other ~3000 endpoints?

Port Response: *Anticipate scanning all Port IP addresses. The Port has approximately 400 external IP addresses, with approximately 20 active and responsive. Internally, assume up to 5,000 endpoints. Items such as switches, IP cameras, etc., were not included in the breakdown. All endpoints are located in facilities owned by the Port: the Oakland seaport, Oakland International Airport (OAK), and the Port's commercial real estate division.*

60. **Supplier Question**: Does the Port have any self-managed cloud assets? If you have cloud assets, where are they hosted? How much (%) of the infrastructure is in the cloud?

    Port Response: *Approximately 10% of the infrastructure is in the cloud.*

61. **Supplier Question**: Does the Port host client data? If so where (cloud, on-prem, or both)?

    Port Response: *In general, no.*

62. **Supplier Question**: Does the Port have remote users and if so, what method are they using to connect to the internal network?

    Port Response*: The Port has remote users who connect to cloud systems and/or use VPN.*

Internal Network Questions

63. **Supplier Question**: Please describe the Port's current backup and recovery environment and methodology?

    Port Response: *Backup and recovery is outside the scope of this engagement.*

64. **Supplier Question**: Can the Port specify the VLAN details, how many are included in the scope?

    Port Response: *Segmentation is in place. Assume approximately 200 segments. Further specifics about the Port's segmentation will be provided once a mutual interest has been established.*

65. **Supplier Question**: Does the Port manage your own Data Center, or do you utilize and 3rd-party/co-location facilities? Are the data centers set up for redundancy between locations, and therefore allowing one location to take on the work of another, or are they all separate datacenters with no backup interaction between each other?

    Port Response: *The Port manages its own data centers. Data center redundancy, failover, etc., are outside the scope of this engagement.*

66. **Supplier Question**: Will all four data centers be accessible from a single location, or will multiple devices need to be deployed to reach the full scope? Are virtual appliances within the data centers possible, such as via NTT remote testing devices (jump boxes)? If not, will a physical device sent to the locations be allowed? Is sampling permitted for networks with similar devices, or will complete penetration testing of all devices be required?

    Port Response*: All four data centers are accessible from a single location, however it is not advisable to scan from one location. Assume two (2) locations for scanning. Virtual or physical appliances can be deployed to facilitate scanning. Regarding sampling, please describe in your plan an approach. A complete penetration test would likely be considered a more thorough approach.*

67. **Supplier Question**: Since a virtualization environment exists, can/will you support a virtualized jump box??

    Port Response*: Yes*

68. **Supplier Question:** How many servers do you have internally (not in the cloud)?

    Port Response: *Assume approximately 90% of the servers listed in the Environment description are physical (not in the cloud).*

69. **Supplier Question:** How many CIDR (Classless Inter-Domain Routing) ranges does the Port have?

    Port Response: *Assume approximately 3.*

70. **Supplier Question**: Is the option to do remote work through an authorized computer, installed on the network by the consultant and subconsultant, an option?

    Port Response: *While an on-premise approach would be preferred, if your approach requires a device on Port premises, that can be accommodated. Please include those details in your response.*

71. **Supplier Question**: Does the Port use SSO or MFA for your current user/system authentication?

    Port Response: *Yes.*

72. **Supplier Question**: What are the Port's disaster recovery strategy and emergency planning documented?

    Port Response: *Disaster recovery and emergency planning are outside the scope of this engagement.*

73. **Supplier Question:** How many IP Cameras and DVRs are in scope?

    Port Response: *Approximately 700 IP cameras and 10 virtual servers recording and managing those cameras.*

74. **Supplier Question:** What security tools does the Port employ (Intrusion Detection, Endpoint Protection, Email Security, etc.)?

    Port Response: *This is sensitive information pertaining to U.S. critical infrastructure and cannot be disclosed at this time. Once a mutual interest has been established, additional details can be provided as necessary.*

75. **Supplier Question**: How many computers are running on a Windows operating system and what is the dominant version?

    Port Response: *Nearly all computers are running Windows. All Windows systems are currently supported Windows versions. The dominant version for servers is currently Windows Server 2012R2 and workstations is Windows 10.*

76. **Supplier Question**: Are all computers to be evaluated running Windows operating system or are there other operating systems in the infrastructure, local or remote? How many Active Directory group policies are in scope for review? Is this a single forest or multi-domain configuration?

Port Response: *The vast majority computers are running Windows, with a small amount of Linux and MacOS. The AD environment is single forest, and there are approximately 75 group policies.*

Web Application Questions

77. **Supplier Question**:

- Do you want a pricing table or for us to scope individual applications? If you would like us to scoping individual applications, please provide the following information for each application.
  - What is the name and purpose of the application?
  - Are these in-house developed applications (by internal or external development teams), or OOB commercial third-party applications?
  - Describe some of the major functionality.
  - How would you describe the complexity of the application?
  - Screenshots (~3-5+) or videos of the application can be provided on the following two pages instead of, or in addition to, answering this.
    - Small – A user can only do a few things once they log in and there is only one user role. These applications are typically less than 10 pages or views in total.
    - Medium – A user can perform several actions and also view various dynamically generated data. There is one or two roles. These applications are typically between 10 and 30 pages or views in total.
    - Large – There is a significant amount of functionality and/or multiple user roles. These applications are typically over 30 pages or views in total.
  - What roles does the application have (e.g. user, manager, admin)? Can the Port describe the difference between these roles?
  - What technologies are in use?
  - If the application is publicly accessible, what are the URL(s) for the application?
  - Is there a standalone API which is not part of web application? If so, please describe it, will documentation for the API be provided?
  - Do these applications utilize RBAC?
  - Are these applications tied to active directory (AD) and/or utilize MFA?

Port Response: *Please describe your approach in your Plan and Approach. While specific application names cannot be provided at this time, anticipate up to 15 web sites or applications to be penetration tested with approximately 100 pages each. Assume up approximately half are unauthenticated, the other half are either SSO with MFA or local login. All environments are production. Assume no APIs, and the applications are written by a third-party provider, so the Port does not have visibility into the source. Please assume up to three (3) roles for each application using the "Medium" to "Large" guidelines above. Credentials will be supplied as required by the supplier's Plan and Approach.*

Virtual Infrastructure Questions

78. **Supplier Question:** For the virtual infrastructure security assessment, does this only include virtualized servers? Is this intended to be an independent configuration review and in scope for the Internal Network Vulnerability Assessment and Penetration Test?

Port Response: *Virtual infrastructure would include all components that make up the virtual environment (e.g., servers, hosts, virtual switches, storage, etc).*

79. **Supplier Question**: Can the Port provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc?

Port Response: *Much of this information is available at the beginning of Section II. Scope of Services. Regarding networking, the Port has approximately 6 Cisco routers, 200 Cisco switches, and 10 firewalls (8 Palo Alto and 2 Cisco). The anti-virus solution is Sophos and the primary database platform is Microsoft SQL Server. Nearly all of the 200 are virtual servers, and are running a supported version of Windows. Of the 200, the breakdown is approximately 10 Domain Controllers, 5 file servers, 10 database servers, and the remainder are largely application servers.*

80. **Supplier Question**: Does the Port use a Virtual Private Network (VPN)?

    Port Response: *Yes.*

Active Directory Questions

81. **Supplier Question**: Is an Active Directory (AD) account going to be provided for certain aspects of testing?

    Port Response: *If an AD account is required, it can be provided.*

82. **Supplier Question**: Active Directory and Group Policy Reviews
    - How many Active Directory forests and domains currently exist within the environment?
    - Does the Port of Oakland use automated workflows to deprovision users leaving the company, including removal from all groups and distribution lists as well as removing remote VPN access?
    - Does the Port of Oakland use automated workflows to delete AD objects that are unused or violate policy, such as user and computer accounts that have not logged in for 90 days?
    - Does the Port of Oakland use the NTLM authentication protocol?
    - Does the Port of Oakland enforce the least-privilege principle, granting users exactly the access they need to do their jobs (no more and no less)?
    - Has the Port of Oakland established a Privileged Access Management (PAM) strategy, where the process of granting and auditing privileged credentials is highly controlled?
    - Is Microsoft Sentinel or any SIEM 3rd party tools currently in use?

    Port Response: *The AD environment is single forest; there are no automated workflows; dormant accounts are addressed but not through automation; NTLM is not being used; least-privilege principles are in effect; PAM principles are in place, and access will be granted as appropriate for assessments; The Port's SIEM is out of scope for this engagement.*

83. **Supplier Question**: Is the target organization's infrastructure centrally managed (e.g., Active Directory, Jamf, etc)?

    Port Response: *Yes.*

Wireless Network Questions

84. **Supplier Question**: Is the goal of this assessment to assess the configuration of all 100 WAPs (Wireless Access Points), or a sample? What is the distribution of the WAPs over the Port's main business facilities? Does a chaperone have to accompany NTT during sampling of wireless traffic from the WAPs?

    Port Response: *Please assume common 802.11x WiFi using predominantly Meraki equipment. If your Plan and Approach requires an on-site walk-through, the Port can provide an escort.*

85. **Supplier Question**: Regarding Wireless Network Assessment and Penetration Testing, does the Port require all sites to be tested?

    Port Response: *Yes.*

86. **Supplier Question**: How many wireless networks are in scope? Include locations, number of SSID's, and ideally what security is in use for each e.g. "Downtown KC office, Corp (WPA2-Enterprise) & Guest (WPA2-PSK) that are in scope of penetration testing?

    Port Response: *Please assume up to 4 SSIDs across 2 locations.*

87. **Supplier Question**: Is the wireless network controller-based or access-point based? Can you please provide the following information: Number of Wireless Device Configurations to Review (NOTE: This should be the quantity of Wireless Controllers, but can be individual APs themselves if uniquely configured and not managed via wireless controller.)

    Port Response: *The Port uses a cloud-based centralized Meraki wireless network.*

88. **Supplier Question**: Will Wi-Fi testing be conducted at each location?

    Port Response: *The three (3) primary business locations described in the beginning of Section II. Scope of Services are in scope for the wireless penetration test.*

Voice over IP Questions

89. **Supplier Question**: Does the Port want a separate report for the VoIP Phone system or as part of the internal/external PenTests? Does the Port want to test all phones, or just a sample of them? What other devices aside from ~750 IP phones make up the VoIP infrastructure?

    Port Response*: The VOIP environment consists of an on-prem Mitel system with ShoreTel VOIP handsets. The VOIP environment is segmented. Both VOIP infrastructure and desk phones are in scope. Please describe your Plan and Approach regarding assessment of the VOIP infrastructure.*

Patch Management Questions

90. **Supplier Question:** Does a patch management program exist? If so, will they be made available for this assessment?

    Port Response: *Yes.*

91. **Supplier Question:** For patch management – what tools are currently used? How many different system groups are individually managed by the solution?

    Port Response: *The primary tool is WSUS. There are approximately 5 workstation and 2 server groups.*

92. **Supplier Question:** Are logs from servers and endpoints being stored in a central syslog server or a SIEM? If a SIEM is in use, which technology vendor is being used? (Splunk, ManageEngine, LogRhythm, Etc.) the server and endpoints currently generating logs? If so, how are they collected and analyzed today?

Port Response: *As this is sensitive information, limited details can be provided at this time. Once a mutual interest has been established, more information can be provided. Presume using logs from central systems in many cases, but local areas in others.*

93. **Supplier Question**: Patch Management:
    1. Is this coordinated with Port IT staff to complete?
    2. Is the patch review for all devices (servers/workstations/networking/voice/network connected devices/IOT)? Please specify systems to evaluate.
    3. Is there 3rd party software that may inhibit patching?
    4. Is an automated patch management solution in place? If so, what solution(s) are in place and will it be reviewed?
    5. Is this review going to be interview-based, reviewing technical configurations of the tool, or a penetration test of the system.
    6. What Patch Management platform(s) are you using? Is it also an RMM platform?
    7. What is your Patch Management process for Windows servers and endpoints? Do you push Windows updates direct from Microsoft or do you have a policy to hold and test?
    8. Are you using a Network Device Management Platform? (i.e. WhatsUp Gold, Solarwinds Network Configuration Manager)
    9. Does the Port use standardized configurations for its IT resources, including routers, user workstations, file servers, etc.)?
    10. Describe the Port test environment. Is every type of platform across the Port represented in the test environment?
    11. Does the Port conduct periodic testing of its backup and restore process to ensure the integrity of backed-up data?
    12. What tools does the Port currently use to monitor security sources for vulnerability announcements, patch and non-patch remediation, and emerging threats?
    13. Can you describe the Port Change and Configuration Management process and communication plan for patch testing and deployment, or provide a process guide?
    14. Are Port patch management procedures and policies well documented? Is there clear ownership within the organization?
    15. Are there any SCCM 3rd party tools currently in use?
    16. Does networking gear use LDAP for credentials?

Port Response*:*

1. *Please describe your approach in your response. Port staff will be made available to discuss if desired.*
2. *All in-scope systems are included in this item.*
3. *In general, no.*
4. *The primary management system is WSUS.*
5. *The Port is open to different approaches. Please describe your approach in your response. A more thorough approach will likely be scored higher.*
6. *The specific tools will be disclosed during the engagement.*
7. *These are specific items that should be discussed and reviewed during the engagement.*
8. *Yes*
9. *Yes*
10. *These are specific items that should be discussed and reviewed during the engagement.*
11. *Backups are not in scope for this engagement. The Patch Management Practices review does not address backups.*
12. *These tools can be disclosed, if appropriate, during the engagement*
13. *This question is more geared for the actual review of the Patch Management Practices*
14. *Yes*

15. *Yes*
16. *This is sensitive information and cannot be disclosed at this time. Once a mutual interest has been established, additional information can be provided.*

Network Questions

94. **Supplier Question**: Regarding Network Configuration Review (including LAN, DMZ, Firewalls and Routers)

- What brands/models does the Port use for your switches?
- What brands/models does the Port use for your routers?
- What brands/models does the Port use for your firewalls?
  - Is the Port using any manufacturer firewall management platforms? (i.e. Cisco Secure Firewall Management Center or Palo Alto Panorama)
  - Is the Port using any 3rd party firewall management platforms? (i.e. Tufin SecureTrack, ManageEngine)
- What is the Port's DMZ configuration? (Single Firewall, Double Firewall, etc)
- How many VLANS are configured? What are they used for?
- How many subnets are configured?

Port Response*: Much of this information is available at the beginning of Section II. Scope of Services. Regarding networking, the Port has approximately 6 Cisco routers, 200 Cisco switches, and 10 firewalls (8 Palo Alto and 2 Cisco). The anti-virus solution is Sophos and the primary database platform is Microsoft SQL Server. Nearly all of the 200 are virtual servers, and are running a supported version of Windows. Of the 200, the breakdown is approximately 10 Domain Controllers, 5 file servers, 10 database servers, and the remainder are largely application servers. Assume approximately 200 VLANs. Details regarding VLANs and DMZ configuration are sensitive information and cannot be disclosed at this time. Once a mutual interest has been established, additional details can be provided as necessary.*

Server and Endpoint Questions

95. **Supplier Question**: Server and Endpoint Log Configuration Reviews

1. Have you deployed any log management tools? (i.e., Papertail, EventLog Manager)
2. What tools are used to store, manage, and search server and endpoint logs?
3. How long does the Port of Oakland keep server and endpoint logs?
4. Does the Port of Oakland periodically review log summary reports for unusual behavior?
5. Who are the recipients of any alerts?
6. Who has administrative access to the logs?
7. What procedures are in place for information governance?

Port Response:

1. *Yes*
2. *This is sensitive information and cannot be provided at this time. Once a mutual interest has been established, additional details can be provided if necessary.*
3. *Assume there are adequate logs to review if needed for the log configuration reviews.*
4. *This is outside the scope of this Request for Proposal.*
5. *This is outside the scope of this Request for Proposal.*
6. *This is outside the scope of this Request for Proposal.*
7. *This is outside the scope of this Request for Proposal.*

96. **Supplier Question**: Server Configuration Reviews, what is the number of Windows Servers by OS version? (2022, 2019, 2016, 2012)? What number of non-windows servers by type does the Port have? (Linux, Unix), and number of Mac OS devices? Has the Port deployed an SCM tool, and if so, which tool(s)? (i.e. Auvik, Ansible)

    Port Response: *All Windows systems are currently supported Windows versions. The dominant version for servers is currently Windows Server 2012R2. SCM tools are out of scope for this engagement. The Proposer is to assess configurations.*

Insurance Questions

97. **Supplier Question**: Does Port require firms to provide the Certification of Insurance with the proposal response?

    Port Response: *No, however proposals are to include Attachment 9 "Insurance Acknowledgement Statement" completed and signed.*

Social Responsibility Questions

98. **Supplier Question**: Please indicate which is the allocated percentage of participation for Small Local Business?

    Port Response: *All firms will be scored in accordance with the Evaluation Weights indicated under Section V. Evaluation Criteria, Item A, Item 5 "Non-Discrimination and Small Local Business Utilization Policy".*

99. **Supplier Question**: Does the prime contractor need to be a SBE or VSBE to respond to this RFP?

    Port Response: *No. Please refer to the Evaluation Weights indicated under Section V. Evaluation Criteria, Item A, Item 5 "Non-Discrimination and Small Local Business Utilization Policy".*

100. **Supplier Question**: Our company has a Small Business Certification with Cal eProcure, does that qualify for the Small Business Enterprise and Very Small Business Enterprise points?

    Port Response: *Please refer to Attachment 5 "Non-Discrimination and Small Local Business Utilization Policy", the twelfth paragraph on becoming Port Certified in the RFP document.*

There are no other questions to RFP No. 22-23/08.