PORT OF OAKLAND

Purchasing Department
530 Water Street
Oakland, CA 94607

Date: **May 20, 2022**

ADDENDUM No. 1

RFP No. 21-22/42 – Payment Card Industry (PCI) Service Provider

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 correction has been made to the above-referenced RFP.

Addition to section "VI. Additional Provisions" Indemnification clause was missing from the RFP when published and is included as follows:

> **Indemnification**
> If Respondent is selected to receive a contract, it will be required to agree to the indemnification clause contained in the Port's Standard Professional Services Agreement. **See Section 5** of the Port' Standard Professional Services Agreement **(Attachment 11)**.

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

1. **Supplier Question**: Does the Port expect 1 or 2 final AOC/ROC(s) as Deliverables for this project?

   Port Response: *Please refer to Section "II. Scope of Services", Item A, Sub-item 3, where "The Proposer shall conduct and complete the Port's PCI-DSS Assessments, scans, and related reports for the duration of the term according to current PCI-DSS Service Provider" are requested. "II. Scope of Services", Item C discusses the term of the expected agreement.*

2. **Supplier Question**: Does the Port require only quarterly ASV scans as part of this project? (i.e. no internal vulnerability scanning or penetration testing of any kind)?

   Port Response: *Please refer to Section "II. Scope of Services", Item A, Sub-item 3, where "The Proposer shall conduct and complete the Port's PCI-DSS Assessments, scans, and related reports for the duration of the term according to current PCI-DSS Service Provider" are requested.*

3. **Supplier Question**: How many external IPs will there be in scope for ASV scanning?

   ***Port Response**: Anticipate scanning all Port External IP addresses. The Port has approximately 400 external IP addresses, with approximately 20 active and responsive.*

4. **Supplier Question**: What is the Port's current annual PCI certification date?

   ***Port Response:** This is not relevant to the proposal. Please refer to Section "II. Scope of Services", Item A, Sub-item 5 for the expected timeline for initial deliverables. This is irrespective of existing or previous certifications by any prior vendor(s).*

5. **Supplier Question**: Are there any Port owned or Port managed infrastructure assets that transmit credit card data? If, "yes" – who is responsible for handling the in-transit credit card data?

   ***Port Response:** Please refer to Section "II. Scope of Services", Item A, Sub-items 1a and 1b.*

6. **Supplier Question**: Is there an incumbent QSA and, if so who is the incumbent and is a copy of the incumbent's latest contract available?

   ***Port Response:** The Port will not be furnishing any information from previous vendor(s).*

7. **Supplier Question**: Are Appendix F contractual terms negotiable?

   ***Port Response:** Please note section "III. Port Policy and Other Requirements", item 5 the last part of the paragraph in **bold** provided here as a courtesy: **Any objections to any provisions in the Port's Standard Professional Services Agreement and/or this RFP must clearly be identified in your proposal**. Changes are discouraged.*

8. **Supplier Question**: Does the Port already have an ASV scanning product that the Port would like the contractor to use for the ASV scans or should that product be included in the proposal?

   ***Port Response:** Please include it in the proposal.*

9. **Supplier Question**: Are required PCI Penetration Tests included in this scope or does the Port have a different vendor providing PCI Penetration tests?

   ***Port Response:** Please include any necessary tests to certify compliance as per Section "II. Scope of Services", Item A, Sub-item 5: "The Proposer shall conduct and complete the Port's PCI-DSS Assessments, scans, and related reports for the duration of the term according to current PCI-DSS Service Provider Level 1 Compliance Requirements".*

10. **Supplier Question**: Is there a not-to-exceed budget for this requirement?

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

11. **Supplier Question**: Given the COVID-19 pandemic, can work be performed remotely to the maximum possible extent?

    Port Response: *Yes, however any testing that requires connectivity to Port systems must be done on site. The Port complies with all state and local mandates regarding COVID-19.*

12. **Supplier Question**: Can we provide the ASV service with the help of a partner?

    Port Response: *The RFP and attachments speak to subcontractors. Please identify any subcontractors and their qualifications in your Proposal as requested.*

13. **Supplier Question**: Apart from the ROC and the quarterly ASV external scans, please confirm if you also need the following:

    - Quarterly internal network scans.
    - Annual external network penetration test.
    - Annual internal network penetration test.
    - Annual segmentation testing.

    Port Response: *Please include any necessary tests to certify compliance as per Section "II. Scope of Services", Item A, Sub-item 5: "The Proposer shall conduct and complete the Port's PCI-DSS Assessments, scans, and related reports for the duration of the term according to current PCI-DSS Service Provider Level 1 Compliance Requirements".*

14. **Supplier Question**: If internal scans/pentests are in scope, how many live internal IP addresses are in scope?

    Port Response: *Approximately 3,000.*

15. **Supplier Question**: If segmentation testing is in scope, in order to gauge the amount of effort that will be needed as part of segmentation testing, can you clarify how many CDE network segments exist and how many non-CDE network segments exist?

    Port Response: *Assume approximately 3 CDE segments and approximately 75 non-CDE segments*

16. **Supplier Question**: Please provide the number of physical locations in scope.

    Port Response*: For Scope Section A, there is one location (Oakland International Airport). For Scope Section B, there can be up to three (3) locations within Oakland.*

17. **Supplier Question**: Apart from port-owned kiosks, terminals, etc. are any applications currently used as well for processing parking payments? Any PA DSS certified applications in use?

    Port Response: *The parking payment application is maintained and certified by the Port's parking provider and is not part of the scope of this RFP.*

18. **Supplier Question**: Please provide a high-level overview of your CDE technical infrastructure with a high-level idea of how many systems are in place and the types/makes of technologies involved.

    Port Response: *For security reasons, the Port cannot release those details at this time. However, from a PCI-DSS service provider perspective, the network environment includes mainstream providers and technologies commonly found at medium to large size airports. Once a mutual interest has been established, more specific details can be disclosed as appropriate.*

There are no other questions to RFP No. 21-22/42.