



State Of Alaska
Department Of Administration
Enterprise Technology Services
333 Willoughby Avenue, 5th Floor
Juneau, Alaska 99811-0206

AMENDMENT NUMBER 3

RFP Title: Payment Card Industry Assessment and Network Scan

Amendment Issue Date: Thursday, March 13, 2008

Request for Proposal Number: 2008-0200-7576

Proposal Closing Date and Time: March 28, 2008, 1:30 p.m.

This Amendment Is Being Issued To:

1. To change closing date and time to that shown above.
2. Answer questions received from potential Offerors.

All terms and conditions not modified by this amendment remain in full force and effect.

A signed copy of this amendment must accompany the proposal or be received by Enterprise Technology Services prior to the deadline set for submission of proposals.

This is a ten (10) Page amendment.

Guy J. Crockroft
Contracting Officer
Phone: 465-5758
Fax: 465-3450
TDD: 465-5745

SIGNATURE

COMPANY NAME

DATE

Question 1: Does the State utilize any other cards such as AMEX and Discover in addition to VISA and MasterCard?

Answer 1: ACCEPTS, the State's credit card program, uses VISA and MasterCard. Other departments may be using other cards.

Question 2: How has the State determined that they are a Tier 3 merchant?

Answer 2: The State Cash Manager confirmed this status.

Question 3: Does the State use a single merchant bank, acquirer, or payment processor? If so whom?

Answer 3: The State uses more than one bank. First National Bank and Keybank are two of the banks that the States currently uses.

Question 4: Have you been audited or been notified that you are going to be audited by Visa or Mastercard?

Answer 4: No.

Question 5: How many external IP addresses in total are in scope? How is this broken out across each of the 16 agencies?

Answer 5: There are a large number of IP addresses. Currently, the State does not have the ability to determine a specific number or the breakdown amongst departments. However, the State believes that credit card processing occurs within approximately 170 different locations (subnets) within our State Wide Networks environment.

Question 6: Must there be coordination with each of the 16 agencies, or a single entity for the scanning?

Answer 6: ETS is the primary customer for the offerer and will be the primary point of contact. ETS will assist with the coordination with the State Agencies, but Offeror will be required to interact with all parties involved.

Question 7: The PCI Data Security Standard requires an annual penetration test and quarterly internal scanning. Is this in scope as well?

Answer 7: Yes. The goal of the State is to have a self-assessment solution to perform a multitude of internal scan requirements that are not required by a third party. The proposed self-assessment solution is independent and is not part of this contract and offerer will be required to perform the scans (internally and externally) to meet the requirements within the PCI standards.

Question 8: Is this the State's first attempt at PCI compliance? If not, what vendor performed the scans the prior year?

Answer 8: This is the State's first attempt, so there is no previous or incumbent vendor.

Question 9: On page 22 of the RFP, Section 2, can you provide additional detail on the type of "self-help" the State is looking for in the portal?

Answer 9: The State is seeking a portal type service or solution to provide assistance for the long-term management, reporting and auditing of the PCI standards.

Question 10: On page 22 of the RFP, Section 2, can you provide additional detail on the type of data or information the State is looking for in the FAQ database?

Answer 10: Since the State has not previously attempted compliance we are unable to answer this question. We are seeking an Offeror with the experience and skills to assist in defining this functionality and to provide answers to the common questions experienced by those attempting to achieve compliance.

Question 11: Can you explain in further detail what the State means by "review network security infrastructure and architecture" in the section "Payment Card Industry Program Management (PCI PM) Deliverables (pages 22-23 of the RFP)?

Answer 11: There are clearly established parameters directly referenced in credit card compliance for infrastructure, architecture and topology. The reference for review only relates directly to those components that are required within the PCI standards.

Question 12: Does the State desire a "Wrap-up Briefing" each quarter after the scans, or one after all of the 16 self-assessments have been completed each year (second major bullet under Payment Card Industry Program Management (PCI PM) Deliverables, pages 22-23 of the RFP)?

Answer 12: Yes, the State will require quarterly briefings. However, Offerors should be aware that the State will also require weekly Project Management reporting and regular progress meetings. The frequency of the progress meetings will be determined by the ETS lead and the assigned Project Manager after an award.

Question 13: How does the State propose to handle "re-scans" to prove compliance for each agency? Should re-scans be included in the pricing? Will the Cost Proposal include optional items?

Answer 13: The State requires the successful Offeror to perform an initial scan and all follow up scans as necessary to prove compliance. Costs for all necessary scans must be included in the Cost Proposal. The Cost Proposal does not include any optional items.

Question 14: Are these weekly calls and all items under the section "Payment Card Industry Program Management (PCI PM) Deliverables" per each of the 16 agencies or for the State management overseeing the compliance efforts?

Answer 14: As per Answer #5, services related to this RFP will be coordinated through ETS.

Question 15: Is there any idea as how many IP address a vendor would expect to run across? Could there be multiple IP address and domains in each Department?

Answer 15: Some departments will have more than one IP addresses. Total public facing IP Addresses for the State is less than 1,000. We have two Class B's, and 21 Class C's inside our network, but not that many devices assigned to the State.

Question 16: It would be helpful to have a maximum number of IP addresses.

Answer 16: More than 65,000.

Question 17: Who is doing the Network scanning now?

Answer 17: The only authorized entity in the State to perform wide-area network scans is the State Security Office (SSO). All external and internal scans will be required to be coordinated with the SSO.

Question 18: Does the State's scanning solution interrogate data? Does it look within application data (repositories)?

Answer 18: Yes, the State's scanning solution does interrogate data and look within application data to a certain degree.

Question 19: It appears to us that this RFP would benefit from accepting responses from Offerors that have subcontractors. This would require a change to Section 1.14 Sub-Contractors. For example, an alliance between a network security company with a financial audit company. Another is a proposal that includes a company that is familiar with the state agencies working on the assessments teamed with a company very experienced in working with PCI evaluations and problem resolutions. With the current requirements we think it would be in the states best interest to be more flexible in their position on subcontractors. Would the State consider allowing subcontractors for this RFP?

Answer 19: Yes. *Delete Section 1.14 in its entirety and replace with:*

1.14 Subcontractors

Subcontractors may be used to perform work under this contract. If an offeror intends to use subcontractors, the offeror must identify in the proposal the names of the subcontractors and the portions of the work the subcontractors will perform.

If a proposal with subcontractors is selected, the offeror must provide the following information concerning each prospective subcontractor within five working days from the date of the state's request:

(a) complete name of the subcontractor;

(b) complete address of the subcontractor;

- (c) type of work the subcontractor will be performing;
- (d) percentage of work the subcontractor will be providing;
- (e) evidence that the subcontractor holds a valid Alaska business license; and
- (f) a written statement, signed by each proposed subcontractor that clearly verifies that the subcontractor is committed to render the services required by the contract.

An offeror's failure to provide this information, within the time set, may cause the state to consider their proposal non-responsive and reject it. The substitution of one subcontractor for another may be made only at the discretion and prior written approval of the project director.

END OF QUESTIONS AND ANSWERS.

Additional Clarifications follow on page 6.

Additional Clarifications:

Replace Section 5 Scope of Work in its entirety and replace with the following:

i. *Compliance Validation Service (CVS)*

The State of Alaska is seeking to gain compliance with the Payment Card Industry (PCI) Data Security Standards, encompassing 16 merchant groups across the state. The State is seeking an authorized Vendor to perform Compliance Validation, Auditing, and Assessment Services to determine areas of non-compliance and help the State develop a plan to achieve and maintain compliance throughout the term of this agreement:

- ❑ Compliance Status – To validate compliance, the State of Alaska requires a letter of compliance to be issued by a Visa Authorized Vendor once all of the State's Merchants achieve compliance with the PCI Data Security Standards.
- ❑ Merchants - To validate compliance, each Merchant requires an annual self-assessment questionnaire and quarterly network scan. Each Merchant will then roll-up to the overall State of Alaska PCI compliance.

In addition, the State is seeking a proposal for a Vendor to provide the ability to manage, track and view compliance status of all merchants enrolled through managed portal service.

Merchant Groups:

The State of Alaska has 16 merchants that need to validate compliance with PCI. These merchants are located throughout the State. Each merchant will validate compliance by completing their own PCI Self-Assessment Questionnaire and having vulnerability scans run against each environment.

The list of merchants is as follows:

- 1) Administration
- 2) Commerce, Community, & Economic Development
- 3) Corrections
- 4) Education and Early Development
- 5) Environmental Conservation
- 6) Fish and Game
- 7) Governor's Office
- 8) Health and Social Services
- 9) Labor and Workforce Development
- 10) Law
- 11) Lt Governor's Office
- 12) Military & Veterans Affairs
- 13) Natural Resources

14) Public Safety

15) Revenue

16) Transportation & Public Facilities

Management Monitoring and Reporting

Vendor will provide a “sponsor” view into the managed solution or portal to allow the State of Alaska the ability to manage the 16 merchants identified under this structure.

Key Management Features must be included:

- ❑ Customizable view
 - The State of Alaska umbrella of merchant groups
- ❑ Executive reporting
 - Most Vulnerable Merchants
 - Supply Chain of Vendors
 - Compliance Statistics
 - Top Vulnerabilities
- ❑ Access to merchant questionnaire and scan data
- ❑ Access to merchant reports and Compliance Certificate
- ❑ View entire merchant population

ii. Per merchant Requirements

1. Vulnerability Scanning Service

- a. PCI requires that all merchants and service providers to complete the PCI self-assessment questionnaire. The solution must provide an easy-to-use portal that satisfies the requirements of all the card associations with self-help and a continuously updated FAQ database.
- b. The solutions must contain an automated vulnerability scanning engine with “Intelligent” scanning that has been tested and determined to be PCI compliant. The State desires to receive monthly scans during the term of the Agreement for up to **(10)** IP addresses per merchant.
- c. Report must be through a secure web interface and provide easy access to concise, auto-generated reports with a high-level summary for executives and managers. The reports must also provide detailed results and remediation action for technicians. Remediation instructions must include CVE-linked vulnerability checks and best practices defined by the security industry.
- d. The infrastructure used in providing the managed service, or portal must be monitored on a 24x7 basis to ensure protection of State data. All State data must be delivered via secure channels.

2. Support must be supplied throughout each phase of the project, Vendor must provide comprehensive online support through the managed service or portal that includes self-help and a continuously updated FAQ database. In addition, email support must be available during standard business hours to answer any questions regarding PCI compliance or vulnerability scanning results.

- **Secure Sockets Layer (SSL) Certificates:** The solution must provide first generation of SSL Certificates encrypts communications between our Web site and our customers at 256 bit. In addition, dual validation is required.

3. Service must include the Trusted Commerce seal.

iii. *PCI Program Management (PCI PM)*

Vendor will assign a PCI Program Managing Consultant to oversee all assessment activities and serve as the primary contact throughout the engagement.

1. The Managing Consultant will coordinate and schedule activities and resources with the State of Alaska
2. Ensure the quality of all Vendor deliverables.
3. The managing consultant will be on-site as needed as well as remote when writing reports and follow-up calls.
4. PM will host weekly calls to identify areas of non-compliance uncovered in the questionnaire and scan results, develop and assist in managing a remediation plan to address the non-compliance issues, validate policies and procedures, and review network security infrastructure and architecture.
5. Based on Vendor will provide comprehensive online support through the portal that includes self-help and a continually updated FAQ database.
6. In addition, email and phone support is required during standard business hours to answer any questions regarding PCI compliance or vulnerability scanning results.

▪ **PCI Program Management will consist at a minimum the following areas:**

- Coordination of completion of questionnaires and timely submittals of questionnaires
- Coordination of External Vulnerability Scanning and to help with scanning remediation
- Instructions for network changes
- PCI DSS verification paperwork

- o Coordinate aggregate of all merchants and submit State wide report to the state and it's acquiring bank(s).
- **Wrap-up Briefing**— Upon completion of the 16 assessments, the Managing Consultant will perform quality assurance on all project deliverables and conduct an informal wrap-up briefing to outline any major issues, point out vulnerabilities uncovered during the course of the assessment and identify any unresolved issues. This briefing will include a discussion of initial findings and proposed recommendations. Any additional products or services performed outside of the initial contract's scope will require an addendum to the contract and additional charges.

Final PCI Reporting- Upon completion of final wrap-up briefing and any last remediation items, a Statewide Certificate of Compliance will be issued by the Vendor.

Cost Proposal
RFP 2008-0200-7576

Offeror Name _____

THIS COST PROPOSAL FORM MUST BE COMPLETED AND RETURNED WITH YOUR PROPOSAL IN A SEPARATE ENVELOPE WITH "COST PROPOSAL" WRITTEN CLEARLY ON THE ENVELOPE, PER THE INSTRUCTIONS FOUND IN SECTION 1.01 OF THE RFP. FAILURE TO DO SO WILL RESULT IN THE PROPOSAL BEING DEEMED NON-RESPONSIVE AND REJECTED.

- A. Enter Total Cost for all deliverables for initial one year term of contract resulting from this RFP as per Section 5.01 Scope of Work, including all related costs

\$ _____

- B. Cost for initial year plus four annual renewal options (multiply above Line A x 5) =

C. Grand Total \$ _____

Costs are for evaluation purposes only.

The lowest 'Grand Total Cost' will receive the maximum number of points allocated to cost (400 points). The point allocations for cost on the other proposals will be determined through the method set out below in Section 2.14, Formula Used to Convert Cost to Points.

I certify the costs contained in this cost proposal have been arrived at Independently, without collusion, and that, unless otherwise required by law, the rates quoted have not been knowingly disclosed prior to award, directly or indirectly, to any other Offeror or to any other competitor.

Signed: _____ Date: _____

Printed name: _____ Title: _____