KENAI PENINSULA BOROUGH SCHOOL DISTRICT

Purchasing Department
139 East Park Avenue
Soldotna, Alaska 99669-7553
Phone (907) 714-8876 Fax (907) 262-7165

ADDENDUM #2

January 27, 2025

TO: ALL PROSPECTIVE BIDDERS

SUBJECT: REQUEST FOR PROPOSAL, #105-25 Cybersecurity Assessment Services

DUE: 4:00 P.M. Alaska Time, February 7, 2025

The following changes, additions and clarifications are hereby made to the subject Invitation to Bid:

RFP 105-25 Pre-Bid Conference
January 17, 2025, 2:00PM Alaska Time
Meeting Minutes

In attendance

Representatives from: Global Solutions Group, InterSec Inc., Plante Moran, ArchTech, Structured Communication Systems, HMH Consultants, Moss Adams, Indrasol, Segal Group, BorderLAN Security, GK Cybersecurity Group, Indusdraw, BPM

For KPBSD: Eric Soderquist, Director of Information Services
Jordan Chilson, IT Manager, Information Services
Kyle Van Ryzin, IT Programmer, Information Services
Colton Hayes, Buyer, Purchasing

Minutes
Eric Soderquist, Director of Information Services opened the Pre-Bid Conference for RFP 105-25 by setting norms and expectations, explaining that a set of prepared slides would be presented, followed by Q&A. Mr. Soderquist explained that each vendor would be given the opportunity to ask one question per question round, and that rounds would repeat, allowing additional questions from vendors, until such time as no further questions existed, or the 1 hour time allotted to this pre-bid conference was reached.

Mr. Soderquist continued with introductions. Present in the room were Eric Soderquist, Director of Information Services; Colton Hayes, Buyer, Purchasing; Jodan Chilson, IT Manager, Information Services; and Kyle Van Ryzin, IT Programmer, Information Services.

Goals and objectives of the pre-bid conference were established. Mr. Soderquist cautioned that we were not going to be sharing operationally sensitive details about our network during the pre-bid or public phase of the RFP and encouraged potential respondents to factor in a "discovery" phase as part of the engagement where such sensitive information could be safely discussed after vendor selection and engagement.

Additionally, a reminder was given that the information shared verbally as part of the pre-bid conference was not to be interpreted as binding. Instead, vendors were encouraged to reference the official RFP documents and any addenda posted to the kpbsd.org Bid Opportunities page.

Mr. Soderquist continued by outlining the section "Background and Organizational Structure" included in RFP 105-25, highlighting details regarding the general IT operation and organization.

A presentation on the goals of this project followed. Mr. Soderquist shared that KPBSD is looking to conduct a cybersecurity assessment that covers a broad range of cybersecurity concerns outlined in the RFP "Scope of Work" item (1). The scope of work presentation also discussed the review of IT Policies and Procedures and recommendations ("Scope of Work", parts (2) and (3)).

Mr. Soderquist covered the "optional services" portion of the RFP by explaining that KPBSD is willing to consider or explore other services typically offered as part of a traditional cybersecurity assessment. Vendors are encouraged to include optional services but should itemize costs for any optional services should they not be included in the base assessment proposal.

Mr. Soderquist explained that the deliverables expected at the conclusion of the cybersecurity assessment include: (1) a confidential assessment report that provides all results of the assessment; (2) a prioritized list of recommendations designed to improve the district's cybersecurity posture; and (3) an executive summary report that does not contain operationally sensitive information that can be shared in public venues.

During the discussion on deliverables, Mr. Soderquist shared some examples of how we envision information to be collected to inform the cybersecurity assessment. Each vendor should provide details on methodology, which may include such elements as IT staff or end user interviews, equipment capabilities/configuration review, review of practices compared to best-practice, sampling of equipment configurations, and/or review of existing policies and procedures.

Mr. Soderquist then shared reminders regarding the RFP process, including key dates, submission guidelines, including a review of Section O (required documentation), and the evaluation criteria and process.

Q&A – Round 1

The following is a summary of questions and answers provided during the pre-bid conference.

Q: Do we need to be in-person for this particular project?

A: There is no requirement to be in-person, but vendors are encouraged to explain in your proposal the methodology by which you plan to gather necessary information to inform an effective cybersecurity assessment.

Q: Can you provide a breakdown of the number of devices, line of business applications, databases?
A: The following are rough estimates of systems most important to our cybersecurity assessment:

- 250-275 managed switches/routers/firewalls
- 40 wireless controllers, 700 access points with centralized policy
- 50-75 physical servers providing infrastructure
- 10-15 Line-of-Business application and/or supporting database servers

Q: Is it safe to assume that configurations are the same throughout, such that a sampling approach is effective?
A: Network routers and switch configurations are generally templated, with each school configured in the same manner as it relates to VLAN configuration, security practices, ACLs, etc. From a line-of-business perspective, it is expected that configuration drift is prevalent.

Q: Are questions going to be posted?
A: Questions period remains open until 4:00PM on January 22, 2025.

Q: What is the budget and timeline for this project?
A: Contracted service engagement must be completed by December 31, 2025. All project invoicing must be submitted no later than January 31, 2026. No specific budget information is available. The contract start date is negotiable but contingent upon grant timelines; it is likely we could be ready as early as March 1, 2025.

Q: Are the devices students take home in scope?
A: KPBSD does not have any formal 1:1 programs or devices. The scope of work specifically identifies concerns related to management of devices as in-scope, including such topics as group policy, and patch management.

Q: Is there any particular security standard you are aligned to?
A: KPBSD is working to align to NIST CSF standards.

Q: Are any line of business applications developed in-house?
A: Yes, KPBSD has one public facing application developed in-house using .NET technologies

Q&A - Round 2

Q: What aspects of cybersecurity assessments are most valuable to KPBSD?
A: The RFP highlights the areas most important to review in the “Scope of Work” section, subpart (1).

Q: Are the business applications hosted on-premises or in the cloud?
A: The majority of application services are hosted on-premises.

Q: Are there any field-work dates that do not work?
A: It is expected that exact timelines would be established during the contracting phase prior to engagement, however, the start of the school year would be less desirable.

Q: Would you allow social engineering in the optional services section?
A: Our primary goal is to conduct a cybersecurity assessment, analyzing existing equipment, configuration, policy and practice. If you offer such additional services, include description and pricing details as part of your proposal.

Q: What do you do for backups?
A: We run routine backups to an enterprise-grade backup platform.

Q: Do you have Data Loss Prevention (DLP)?
A: We are not prepared to share specific details. If your proposal includes evaluation of Data Loss Prevention, include such specifics in your proposal.

Q: Do you run your own phishing campaigns?
A: We are not prepared to share specific details. If your proposal includes evaluation of best practices around user training in topics such as phishing, include such specifics in your proposal.

Q: Do you anticipate having dedicated time for collaboration and interviews? If so, around how many hours?
A: Information Services is prepared to dedicate the necessary team member(s) needed to ensure this assessment is successful.

Q&A – Round 3

Q: Do you use Endpoint Detection and Response?
A: We are not prepared to share specific details. If your proposal includes evaluation of Endpoint Detection and Response, include such details in your proposal.

Q: What are the long-term cybersecurity goals?
A: Long term goals are to align operational practices and procedures to NIST CSF.

Q: Are there any specific threats you are most concerned about?
A: There is nothing specific identified.

Closing
Mr. Soderquist thanked participants for taking time to participate and learn more about the KPBSD cybersecurity assessment practices. Participants were reminded that any further questions can be emailed to the KPBSD purchasing department via email contacts included in the RFP Instructions to Bidders. Questions received will be answered no later than 10-days prior to closing of the RFP. Participants were also reminded that the submission deadline for this RFP is 4:00PM Alaska Time on February 7, 2025.
In closing, Mr. Soderquist shared that minutes from the pre-bid conference would be made available.
The pre-bid call concluded at approximately 2:45PM Alaska Time

NOTE TO BIDDERS: Please sign and return one (1) copy of this sheet with your Bid to acknowledge receipt of Addendum #2 REQUEST FOR PROPOSAL: #105-25

BIDDER: _____

(Firm Name)

Mailing Address: _____

Date: _____

Signed by: _____

(Signature and Title)