KENAI PENINSULA BOROUGH SCHOOL DISTRICT

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

ADDENDUM #3

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:

The following questions were received:

Q: Would an email submission be accepted instead of mail?

A: See RFP Instructions to Bidders for all submission requirements.

Q: Please provide any recording or notes from the pre-bid conference if available.

A: All addendums, including meeting minutes from the pre-bid conference, are available on the KPBSD Bid Opportunities page at https://kpbsd.org/departments/assistant-superintendent/instructional-support/planning-and-operations/purchasing/bid-opportunities/

Q: Is there a contract the chosen vendor is expected to sign governing the engagement or should vendors include a sample copy of our version?

A: KPBSD and the chosen vendor will collaborate to assemble contract language following award that outlines mutually agreed upon terms between both parties as well as those specified by the State of Alaska Division of Homeland Security & Emergency Management's State and Local Cybersecurity Grant Program.

Q: A section M.2.G is referenced in the RFP, but may be missing. Where can section M.2.G be found?

A: See page 6 of the RFP Instructions to Bidders.

Q: Are the certificates of insurance to be provided in the RFP response or rather, on award?

A: Certificates of insurance are to be provided upon award, as requested by the District.

Q: What operating systems are used and what are their versions?

A: Primarily Windows 10 and Chrome OS for client devices with some Mac OS and iPad OS devices at select schools (assorted versions).

Q: What is the current patch management process and frequency?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What security measures are currently in place for critical applications?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What data and backup solutions are in place?

A: KPBSD utilizes an enterprise backup solution. Beyond this high-level description, KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Are there any data loss prevention measures in place?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Does KPBSD have a documented disaster recovery plan and has it been tested?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What is the allocated budget for this cybersecurity assessment?

A: KPBSD intends to fund this project through a grant opportunity, and we are committed to ensuring responsible use of these funds for the district's cybersecurity assessment needs. Our priority is to select a proposal that meets the objectives outlined in the RFP in a fiscally responsible manner. As such, we are seeking comprehensive solutions tailored to our specific requirements for an organization of our size. KPBSD does not intend to release a specific budget number to ensure that proposals remain competitive and reflect unbiased pricing.

Vendors are encouraged to provide detailed breakdowns of costs associated with the project. This will allow us to fully evaluate the value and scope of services provided. Proposals should reflect the actual costs of delivering the services as described. Cost is the largest weighted factor in our evaluation process and will be considered alongside other critical elements such as methodology and experience.

Q: What is the desired timeline for the assessment and required deliverables?

A: Contracted service engagement must be completed by December 31, 2025. All project invoicing must be submitted no later than January 31, 2026. 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: What specific NIST framework is KPBSD aiming to align to?

A: NIST CSF

Q: What is the desired timeline for achieving NIST compliance?

A: There is no specific timeline established.

Q: Is information security documentation available upon request? How many pages are currently maintained/utilized?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Is technical documentation (network architecture, Visio designs, process documentation, etc.) available upon request? How many pages of technical documentation are available?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Is a disaster recovery plan documented and formalized?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Are there incident response procedures in place?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: How many total devices of each type are on your network (physical servers, virtual servers, workstations, printers, IP phones, network devices, IoT devices, etc.)?

A: The following are approximate counts of active devices based on type:

- Servers: 50-75 physical servers
- Virtual Servers: 150-200
- Client Devices (Desktop/Laptop/Chromebook): 8,000-9,000
- Printers: 700-800
- IP Phones: Approximately 1,400
- Managed Network Devices:
    - Switches/Routers: Approximately 250
    - Wireless Controllers: Approximately 40
    - Access Points: Approximately 800

Q: How many firewalls are in scope?

A: KPBSD utilizes firewalls in multiple locations within our infrastructure, both dedicated firewall equipment as well as software-based firewalls. Evaluation of operational practices related to this equipment is in scope. Beyond this high-level description, KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Are any load balancers in scope?

A: Yes, many of our line-of-business applications utilize load balancers.

Q: Are any firewalls in paired/HA mode?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: How many line-of-business applications are in scope?

A: We have 10-15 line-of-business applications, each consisting of application, database, and in some cases, load-balancing or other supporting infrastructure.

Q: Can a detailed network diagram, including network segmentation, firewall placements, and connections be provided?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What are the current security configurations for devices connected to the network (e.g. default passwords, firmware updates)?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Can you specify the VLAN details, including the number of VLANs included in the scope of work?

A: KPBSD utilizes VLAN segmentation across our user-facing and server networks. Each LAN typically has fewer than 15 total VLANs, and the general purpose of each VLAN is generally consistent between different locations. Beyond this high-level description, KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What is the age and condition of the network infrastructure (routers, switches, wireless access points)?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What security measures are currently in place for the Soldotna data center (physical security, access controls, redundancy)?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Do you manage your own datacenter, or do you utilize any 3rd-party or colocation facilities?

A: KPBSD manages equipment in our own datacenter. We do not presently rely upon 3rd-party or collocated services for infrastructure services.

Q: Can KPBSD provide more detail on the shared resources and interdependencies with KPB?

A: KPBSD maintains and manages equipment that provides a single internal network peering point with KPB. No KPB-owned assets, processes, or procedures are in-scope to this project. This cybersecurity assessment is limited to equipment and configuration managed by KPBSD that facilitates this peering arrangement.

Q: Will KPB be involved in any part of the assessment or remediation process?

A: No. The assessment and remediation process should focus on KPBSD owned and managed assets, processes, and procedures.

Q: What endpoint detection and response solutions, if any, are currently deployed?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: How much of the infrastructure is in the cloud?

A: KPBSD does not directly manage any PaaS or IaaS services.

Q: How is Amazon Web Services used in the organization?

A: Amazon Web Services is not utilized.

Q: How is Microsoft Azure used in the organization?

A: Microsoft Azure is utilized primarily for identity services.

Q: How is Google Cloud Platform used in the organization?

A: Google Cloud Platform is used for limited OpenID authentication services for fewer than five authentication flows.

Q: Are other cloud services (e.g. OVH, Rackspace, etc.) used in the organization?

A: No.

Q: How many IP addresses have been assigned to you by Cloud Service Providers?

A: None.

Q: What Microsoft 365 licenses are currently in use?

A: Most staff are licensed with Microsoft A3 or better. KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: How many conditional access policies are present?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: How many users are in the tenant?

A: The majority of our staff and student population utilize Microsoft 365 in varying capacities.

Q: How many MDM policies and profiles exist?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity

assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: What is the expected level of on-site assessment activities?

A: There are no specific requirements regarding on-site engagement. As outlined in the Evaluation of Proposals section of the RFP Instructions to Bidders, proposals will be scored, in part, on the methodology proposed, with consideration of elements such as work plan design, service efficiencies, and overall cost of benefit to the project.

Q: Would a 100% remote provider's proposal be negatively scored?

A: There are no specific requirements regarding on-site engagement. As outlined in the Evaluation of Proposals section of the RFP Instructions to Bidders, proposals will be scored, in part, on the methodology proposed, with consideration of elements such as work plan design, service efficiencies, and overall cost of benefit to the project.

Q: Will provider tools be allowed on the network for information gathering?

A: Potentially based on the level of access needed. Work requiring direct network access in lieu of relaying through KPBSD IT staff should be outlined in your proposal.

Q: Are there any specific areas of concern or areas KPBSD wants to prioritize for improvement?

A: See RFP Scope of Work, Items 1a-g, and Items 2a-c

Q: What criteria will KPBSD use to evaluate and prioritize the recommendations?

A: Recommendations should be prioritized in the final reports to KPBSD based on the professional experience of the assessors.

Q: Is it the intent of the district to implement security recommendations in-house using the results of the assessment, or to have an outside firm implement recommended security-related findings?

A: It is expected that many security recommendations will be implemented in-house, however, KPBSD may elect to engage external resources if considered necessary.

Q: How many employees work in the IT department?

A: There are 14 IT employees.

Q: How many staff members are dedicated to cybersecurity?

A: The security team consists of 5 members, with each having other IT responsibilities.

Q: Is there an incumbent or previous incumbent who completed similar contracts performing cybersecurity assessment services?

A: No.

Q: Are you interested in a WiFi assessment?

A: WiFi performance assessments are outside the required scope of this project. Proposals for optional services should contain detail and pricing for various options proposed.

Q: Is wireless testing in-scope? If so, is the wireless network controller-based?

A: Analysis of wireless infrastructure security practices is included in the scope of work (see RFP Scope of Work #1a). The wireless platform is controller-based.

Q: What type of penetration testing is preferred?

A: Penetration testing is not a required scope for this project. Proposals for optional services should contain detail and pricing for various options proposed.

Q: Are there any specific systems or applications that KPBSD wants to prioritize for penetration testing?

A: Line of business applications would be primary. Additional systems would be at the recommendation of the assessor.

Q: Are both internet and external networks included in the optional penetration testing?

A: Penetration testing is not a required scope for this project. Proposals for optional services should contain detail and pricing for various options available.

Q: How many active public IP addresses are in scope for penetration testing?

A: It is estimated that no more than a /22 worth of public address space would be in-scope for external penetration testing.

Q: How many active internal IP addresses are in-scope for penetration testing, and can the network be tested from a single location?

A: Specific internal IPs active varies. Testing from one or multiple locations would be determined based on recommendations of the assessor following discussions on the design of our network to be conducted during the initial phases of the assessment.

Q: Is application layer web application testing included in scope? If so, how many applications? Will credentials be provided for authenticated testing?

A: Application layer web testing is not a required scope for this project. Proposals for optional services should contain detail and pricing for various options available.

Q: Please list the physical locations you plan to include in the Physical Security Assessment portion of the proposed project.

A: No physical security assessments are included in the required scope of work.

Q: What cybersecurity awareness training is provided to staff and students?

A: KPBSD considers details regarding the configuration or deployment of this topic to be operationally sensitive. Once a contractual agreement is in place with a cybersecurity assessment provider, we are prepared to collaborate and share the necessary information to support the assessment.

Q: Is social engineering testing in scope?

A: A review of practices and procedures related to social engineering tactics is in-scope, but performing live social engineering testing is outside the required scope of this project.

Q: Are you interested in phone-based or email-based social engineering?

A: A review of practices and procedures related to social engineering tactics is in-scope, but performing live social engineering testing is outside the required scope of this project.

Q: Are all employees considered in-scope for this assessment?

A: A review of practices and procedures related to social engineering tactics is in-scope, but performing live social engineering testing is outside the required scope of this project.

Q: Is your objective to assess overall employee awareness, or more tailored to spear phishing that targets select individuals with different content and delivery methods?

A: A review of practices and procedures related to social engineering tactics is in-scope, but performing live social engineering testing is outside the required scope of this project.

NOTE TO BIDDERS: Please sign and return one (1) copy of this sheet with your Bid to acknowledge receipt of Addendum #3 REQUEST FOR PROPOSAL: #105-25

BIDDER: _____

(Firm Name)

Mailing Address: _____

Date: _____

Signed by: _____

(Signature and Title)