ADDENDUM 1
KODIAK ISLAND BOROUGH
KIB Cybersecurity Infrastructure Project
Kodiak, AK

August 28, 2025

TO ALL PLAN HOLDERS OF RECORD:

This addendum forms part of and modifies the contract documents as noted below. Bidders must acknowledge receipt of this addendum in the space provided on the Acknowledgement of Addenda form which can be found on page 14 of this RFP. Failure to do so may submit Bidder to disqualification.

This addendum consists of 5 pages.

IMPORTANT DATES are updated to be written as follows to allow for more time for questions (updated dates are in bold):

Issue Date:	August 8th 20205
Questions Deadline:	**September 12th, 2025**
Proposal Deadline:	**September 26th, 2025**
Proposal Evaluations:	**November 7th, 2025**
SLCGP approval	TBD
Notice of Intent to Award:	TBD
Protest Period:	TBD
Anticipated Contract Approval:	TBD

Answers to questions regarding the RFP:

Firstly, I have a purely administrative question. If a firm has "registered" on the Kodiak web portal (https://kodiakak.us/bids.aspx?bidID=121), do they still need to submit the printed "registration form" in order to receive addenda and budget information?

Yes, please submit the printed "registration form" in order to receive addenda and budget information

Please clarify the deadline for questions. (It is listed on page 12 as August 29, 3:00 PM, and on page 4 as September 5.)

The deadline is September 12th, 2025

The RFP requests a phased timeline to complete the project by June 30, 2026, but the award and contract approval date are "TBD." What should we use as an anticipated Notice to Proceed date for our schedule?

The internal scoring of submitted RFP's will take 45 days, however once a contractor is selected, they MUST be reviewed and approved by the Alaska Division of Homeland Security and Emergency Management Grants Section in Juneau, which will take an unknown time.

Can proposals be submitted only by email, or do we need to submit a hard copy even if we email our proposal?

KIB code requires that proposals be received by delivery in a sealed proposal package. Proposals must include one hard copy original, and one exact digital copy on a USB flash drive, and be submitted by courier, or U.S. Mail, clearly addressed, and in sealed envelope or box.

With respect to the Alaska business license requirement, please confirm that this is not required at bid time, and that the selected contractor can obtain this license after award, prior to signing the contract.

You are correct that it is not required at bid time, but must be obtained after award, and prior to signing the contract.

Per paragraph E of the proposal documentation instructions, please provide us with the final project budget.

The grant funds awarded by the State and Local Cybersecurity Grant Program (SLCGP) is for $225,000

The scope of work refers only to installing and configuring equipment. Will the contractor also be responsible for purchasing the equipment within the contract price?

The contractor also will be responsible for purchasing the equipment within the contract price.

Will the Borough provide any in-house “smart hands” for physical tasks such as racking and stacking, cabling, mounting wireless APs, etc., or should we assume the contractor will be fully responsible for those tasks?

The Borough will provide any in-house “smart hands” for physical tasks such as racking and stacking equipment, cabling, and amounting devices.

Please clarify the number of firewalls required. The introduction to paragraph 1of the scope of work states 4, but the sub-paragraphs require “redundant” firewalls at both the main site and 3 satellite locations, which would be 8.

The main site requires redundant firewalls, as well as one satellite location, with the remaining two satellite locations do not require redundancy for a total of six firewalls.

Please clarify whether the Borough has a preferred vendor or OEM for the firewalls and switches to be installed. Will the new equipment need to interface with any legacy network infrastructure (e.g., switches, firewalls, controllers, or monitoring systems)?

The Borough does not have a preferred vendor or OEM for the firewalls and switches to be installed. The new equipment will need to interface with a legacy Dell S4048.

If it is not feasible to provide all requested equipment within the stated project budget, would the Borough prefer a proposal that (a) exceeds the budget in order to fulfill the full equipment list, or (b) adjusts the quantity or specifications of equipment to remain within budget? Would the Borough be amenable to option pricing and/or alternate proposals in this case?

The Borough would adjust the quantity or specifications of equipment to remain within budget.

Regarding the remote access and ZTNA requirements outlined in Section D.6 of the Scope of Work: Is the Borough specifically seeking a commercial ZTNA solution (e.g., Zscaler or similar), or would the Borough consider solutions that implement Zero Trust principles using other architectures (e.g., policy-based access control, ACLs, and role-based segmentation)?

The Borough will consider both types of proposals, one which leverages the built-in capabilities of the vendor's firewalls, and one that utilizes a range of other architectures. The solution must be available to be used by our mobile clients such as iPads and other mobile devices.

The RFP references Industrial Systems Security (ICS) and SCADA capabilities in Sections 1.b.i and 4.a. We have a few clarifying questions:

- Is the contractor expected to simply provide a network solution with ICS/SCADA-compatible capabilities, or will we be responsible for configuring these features to actively interface with the Borough's ICS/SCADA systems?
- To ensure compatibility, could the Borough provide an inventory of current ICS/SCADA devices, including make/model, protocol(s) in use, and network placement?
- If configuration is required, will this involve only integration with existing ICS/SCADA devices, or will new industrial assets be introduced as part of this project?
- If configuration is required, will the contractor's role be limited to configuring the network to observe ICS/SCADA traffic, or will we be expected to directly interact with or configure the ICS/SCADA devices themselves?
- Are there any constraints, safety protocols, or approved maintenance windows we should be aware of related to the ICS/SCADA equipment that may impact available work windows or efficiency?

The contractor is expected to simply provide a network solution that protects and includes our minimal SCADA systems within the management and security analytics platform listed in the RFP at D-4. This will include the configuration to observe SCADA traffic.

Can the Borough clarify whether the 75 endpoint licenses are intended to cover only traditional user devices (e.g., laptops, desktops, servers), or if they also include IoT devices or ICS/SCADA systems?

The 75 endpoint licenses referenced are all traditional user devices such as workstations, servers, laptops, iPads, and mobile phones such as iPhones and Samsung Galaxies. No SCADA systems.

The SOW introduction (paragraph A) mentions training, but this is not included in the expanded scope of work (paragraph D). Will the contractor be expected to provide technical training for Borough IT staff as part of the implementation, or is user/administrator training out of scope? If so, can you provide more details regarding the Borough's expecations for this scope of work?

The Borough is looking for standard user/administration training of the new equipment, interfaces, and software.

Does the Borough expect the selected contractor to provide any ongoing support, maintenance, or monitoring services after initial deployment, or is the scope limited to one-time implementation and configuration?

The scope of this RFP does not include ongoing maintenance and is a one-time implementation and configuration.

Does your budget include the cost all hardware and subscriptions? (The RFP reads like it does, just wanted to confirm.)

Yes, the budget includes the cost of all hardware and subscriptions.

The RFP on page 5 indicates that the scope of this project is the "Installation and Configuration". We would like to confirm that the scope does not include the purchase of these hardware devices, and only is for the installation and configuration of hardware devices that KIB will furnish?

The scope of the project includes the purchase of the hardware devices, as well as the installation and configuration of those hardware devices.

The RFP on page 5 indicates "Install and configure 4 redundant next-generation firewalls at 4 locations"; however, 1.a and 1.b indicate a total of 5 NGFW's and not 4. Please clarify.

The project requires two redundant firewalls at the main KIB location, and a single firewall at three satellite locations each for a total of five Next Generation Firewalls.

Will there be a need run any additional network cables or are they already in place? (cable runs for access points)

This project scope does not include any additional cable runs, and most cables are in place. Should there be any need for additional cabling, KIB staff will provide them.

Are their specific carriers desired for use in the LTE modems?

The Kodiak region has two carriers that KIB will accept: either Alaska Communications Service (ACS), or General Communications Inc. (GCI)