ALASKA RAILROAD CORPORATION
327 W. Ship Creek Ave.
Anchorage, AK 99501
Phone 907.265.2593
GOEMERG@AKRR.COM

April 17, 2023

Addendum 1
RFP #23-22-210719
SIEM Software, Hardware, Implementation Training and Integration Services

Addendum number 1 has been issued for questions/ clarification.
The Closing Date for this ITB has changed.
Proposals will be received until May 9, 2023 @ 3:00 PM Alaska time.

Questions:

1. Is Alaska Railroad able to provide an extension to the response deadline?
   a. Yes the new closing date will be May 9, 2023

2. We understand that Alaska Railroad is seeking to procure the entire managed suite of security tools that encompasses people and expertise from a single vendor. In the event that a vendor can only provide a subset of the entire scope of services, is Alaska Railroad willing to consider single set solutions where the vendor could be included on the team with the selected contractor?
   a. Yes. This is the purpose of having 3 parts, where a firm may be best qualified/suited for only one part, or many parts.

3. Are vendors allowed to submit bids with multiple firms included in the same proposal? If yes, does only the prime contractor need to complete Sections E&F, or does both the prime and all sub-contractors required to complete Sections E&F?
   a. Yes, only the prime contractor needs to complete Sections E & F.

4. Could you provide a network TAP in one or a few area's of the network to see all Vlans?
   a. Yes

5. Will you be providing a Network Diagram?
   a. No, but I can provide spoken details of the architecture to satisfy your needs. You can also bid based on air-gapped / fully segmented / untrusted areas of the network that may require their own TAP or device.

6. Are you looking for Virtual NDR for cloud providers (Google/Azure/AWS)?
   a. Possibly, it depends on price, functionality, integration, etc.

7. Will you require decrypting functionality?
   a. Please bid on this separately. We may require it in some segments.

8. Do you have a current EDR vendor? How many hosts/endpoints in your environment?
   a. No

9. Do you currently have a SIEM/SOAR vendor to utilize?
   a. No

10. How many events per second (EPS) or GB/Day will you be sending to the scoped solution? If unknown, we can estimate EPS and GB/Day based upon our experience and previous calculations.
    a. We expect to have a maximum 3000 EPS

11. Where is your infrastructure located and what percentage resides at each location? (Example: Azure 50%, GCP 10%, AWS 20% and OnPrem 20%)
    a. IT. 99% On Prem. 80% in anchorage, with 20% from Seward to Fairbanks.
    b. OT. On Prem, With 50% in Anchorage, and 50% spread from Seward to Fairbanks.

12. How many ingress/egress points does the company have on the network?
    a. Currently 3, but there may be an expansion.

13. Where are these ingress/egress points physically located?
    a. Anchorage

14. What is the average and maximum network bandwidth at these locations, Mbps or Gbps?
    Unix or Linux Servers, Windows Active Directory, Windows IIS/Exchange, Windows General Purpose, Web Servers, Proxy Severs, AV Servers, NAS (mostly Synology), Database Servers, DNS and DHCP Servers, Routers and Switches, Firewalls, IDS or IPS, VPNs
    a. Currently we have ~500Mbps ingress/egress bandwidth.
    b. Network traffic may have a 5GB/s average, with 300GB/s across all routers simultaneously.

15. What additional SaaS based services would you like to collect from? (Example: Cloudflare, Salesforce, Jamf, O365)
    a. Cloudflare, salesforce, O365. We have limited interactions with those currently, but O365 will grow.

16. What are your log retention requirements (3 months, 6 months, 12 months are common)?
    a. 12 Months of aggregated logs, 3 months of raw logs.

17. Do you currently have a Network TAP Packet Broker- invested solution or preference (Gigamon, Keysight Ixia, Garland, Niagra Networks) deployed that you want to integrate with NDR ?
    a. No.

18. Which compliance requirements is your business subject to? Will you be using the Cyber solution to meet compliance requirements?
    a. TSA SD 1580/82-2022-01
    b. Positive Train Control
        i. PTC may be voluntarily developed and implemented by a railroad following the requirements of 49 Code of Federal Regulations (CFR) Part 236, Subpart H – Standards for Processor-Based Signal and Train Control Systems; or, may be as mandated by the Rail Safety Improvement Act of 2008 developed and implemented by a railroad following the requirements of 49 CFR Part 236, Subpart I – Positive Train Control Systems.
        ii. 49 CFR §236.921 Training and qualification program, general.
        iii. 49 CFR §236.925 Training specific to control office personnel.
        iv. 49 CFR §236.1033 Communications and security requirements.
        v. 49 CFR Part 236 Appendix B - Risk Assessment Criteria
        vi. 49 CFR §236.18 Software management control plan.

c. PCI (some segments)
d. HIPAA
e. **Executive Orders for Critical Infrastructure: 13231, 13636, 13800**
f. **Executive Order refers to the NIST Cybersecurity Framework:**
    i. NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations (Current Version)
    ii. NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security (Current Version)
    iii. PCI-DSS Payment Card Industry – Data Security Standards (Current Version)
g. **Breach Notification Requirements**
    i. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
    ii. **Alaska**: http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx09/query=[JUMP:%27AS4548010%27]/doc/{@1}?firsthit
    iii. **HIPAA**: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
    iv. **PCI**: https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf
    v. **DHS**: https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017.pdf
h. Yes, we will need the respondent to help us ensure we meet our regulatory requirements.

Clarifications:

Please update the Service Bid Form Section E, in its entirety with the one attached herein.

Attached herein is the Sizing document referenced on page 9 as (Attachment 3) but was not provided. Additionally we have included the TSA Security Directive, NIST 53 and 82 Guidance that was listed as Attachment 4.

An Excel copy of the PDF Attachments will be available and will be sent out using a Dropbox link to the email contacts listed on cover page response used to register for the pre-proposal conference after conclusion of the pre-bid meeting.

Please acknowledge receipt of this and all addendums in your firm's Service Bid Form. All other terms and conditions remain unchanged.
If there are any questions regarding this addendum please let me know.

Thank you,

Greg C Goemer
Sr. Contract Administrator
Alaska Railroad Corporation

Sizing

Events & Storage	
Device Type	**Quantity**
Windows Active Directory Servers	8
Windows IIS and Exchange Servers	6
Windows General Purpose Servers	500
UNIX and Linux Servers	400
DNS and DHCP Servers	8
Antivirus Servers	4
Database Servers	18
Proxy Servers	2
Large Firewalls	10
Small Firewalls	10
IDS, IPS, and DAM	3
VPNs	10
Access Points, Routers and Switches	150

Flows	
Device Type	**Quantity**
Total Workstations on Network	750
Total Servers on Network	2000

NetFlow	
Type & Bandwidth	
Number of Internet Connections	5
Total Bandwidth of Internet Connection	600Mb
Typical Bandwidth between any Remote Sites	300MB

Additional Log Sources	
Device Type	**Quantity**
IBM i	12
HP SAN	15
Wireless	50
SCADA	1500

PTC related Log Source Sites and Equipment	
Device Type	**Quantity**
Cisco Switches / Routers (May need to be captured at ASA location in main facilities)	145
IP Phone/IP Radio (May need to be captured at ASA location in main facilities)	111
Battery Backups (May need to be captured at ASA location in main facilities)	111

Note:
Logs will be pulled from most workstations and servers once per minute

5. Please provide any long-term data retention needs including compliance (e.g., 1 year for PCI-DSS):	13 Months
6. Please indicate any cloud hosted software with the numbers of users (e.g., Microsoft 365, 200 users):	O365 - 200

TSA Security Directive Requirements					
	Product completely addresses	Product partially addresses	Product does not address	Notes on Product/Service Implementation	Notes on Alaska Railroads approach
Note: each product does not need to accomplish all aspects of the Security Directive. Each product will address one or more aspects, and the award will include complimentary products that fulfill all areas of these requirements.					
A. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice-versa. As applied to Critical Cyber Systems, these policies and controls must include:					We are planning the implementation of various firewalls to segregate the network.
1. A list and description of:					
a. Information Technology and Operational Technology system interdependencies;					ARRC will need help from various products to assess our segregation and detail the allowed communications.
b. All external connections to the Information Technology and Operational Technology system;					Products will need to be aware of the definition of IT vs OT and differentiate between them.
c. Zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity; and					ARRC will accomplish this with firewalls, and define the zone boundaries based on IT/OT and CCS related attributes.
d. Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.					ARRC will implement Firewalls for this.
2. An identification and description of measures for securing and defending zone boundaries, that includes security controls:					Each product should reflect some capabilities for this item.
a. To prevent unauthorized communications between zones; and					Most products will help stop, identify, report on, or respond to an anomaly that arises in this area.
b. To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.					Product restrictions may apply in this area. If a product contains IT content, entry
B. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:					Products will need to implement 2FA or assure that a 2nd factor is present prior to use.
1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include:					All products should have some comment on this requirement.

TSA Security Directive Requirements					
	Product completely addresses	Product partially addresses	Product does not address	Notes on Product/Service Implementation	Notes on Alaska Railroads approach
a. A policy for memorized secret authenticators resets that includes criteria for when resets must occur[10]; and					All products should have some comment on this requirement.
b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (III.CJ .a), and a timeframe to complete these mitigations.					All products should have some comment on this requirement.
2. Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.					Products will need to implement 2FA or assure that a 2nd factor is present prior to use.
3. Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.					All products should have some comment on this requirement.
4. Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure:					All products should have some comment on this requirement.
a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and					All products should have some comment on this requirement.
b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.					ARRC uses policy and procedure to enforce this.
5. Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.					ARRC uses policy and procedure to enforce this. Products should highlight where a firewall and zero domain trust will affect their implementation.
C. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and c01Tect anomalies affecting Critical Cyber Systems. These measures must include:					All products should have some comment on this requirement.
1. Capabilities to:					
a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;					Some products should have some comment on this requirement.
b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;					We use firewalls to accomplish this.

TSA Security Directive Requirements					
	Product completely addresses	Product partially addresses	Product does not address	Notes on Product/Service Implementation	Notes on Alaska Railroads approach
c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;					We use firewalls to accomplish this.
d. Block and prevent unauthorized code, including macro scripts, from executing; and					All products should have some comment on this requirement.
e. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).					All products should have some comment on this requirement.
2. Procedures to:					
a. Audit unauthorized access to internet domains and addresses;					All products should have some comment on this requirement.
b. Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;					Some products should have some comment on this requirement.
c. Identify and respond to execution of unauthorized code, including macro scripts; and					All products should provide comment on this requirement.
d. Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.					
3. Logging policies that:					
a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and					All products should provide comment on this requirement.
b. Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.					All products should provide comment on this requirement.
4. Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.[11]					Some products should provide comment on this requirement.
D. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk based methodology. These measures must include:					Some products should provide comment on this requirement.
1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.					Some products should provide comment on this requirement.
2. The strategy required by section III.E.l. must include:					

TSA Security Directive Requirements					
	Product completely addresses	Product partially addresses	Product does not address	Notes on Product/Service Implementation	
a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and					
b. Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.[12]					
3. If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.					
E. Develop a Cybersecurity Assessment Program for proactively assessing and auditing cybersecurity measures.					
1. The Owner/Operator must develop a Cybersecurity Assessment Program for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.					
2. The Cybersecurity Assessment Program required by Section III.F.1. must					
a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;					
b. Include an architectural design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. An architectural design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and					
c. Incorporate other assessment capabilities designed to identify vulnerabilities based on evolving threat information and adversarial capabilities, such as penetration testing of lnformation Technology systems, including the use of "red" and "purple" team (adversarial perspective) testing.					

12 Available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

SECTION E

ALASKA RAILROAD CORPORATION
SERVICE BID FORM of:

NAME _____

ADDRESS _____

_____

To the CONTRACTING OFFICER, ALASKA RAILROAD CORPORATION:

In compliance with your Request for Proposal No. 23-22-210719, dated 4/6/2023, the Undersigned proposes to furnish and deliver all the services and perform all the work required in said Invitation according to the scope of work and requirements contained therein and for the amount and prices named herein as indicated on the Cost Proposal.

The Undersigned acknowledges receipt of the following addenda to the requirements and/or scope of work for this Request for Proposals (give number and date of each).

Addenda Number	Date Issued	Addenda Number	Date Issued	Addenda Number	Date Issued

NON-COLLUSION AFFIDAVIT

The Undersigned declares, under penalty of perjury under the laws of the United States, that neither he/she nor the firm, association, or corporation of which he/she is a member, has, either directly or indirectly, entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competitive bidding in connection with this proposal.

The Undersigned has read the foregoing proposal and hereby agrees to the conditions stated therein by affixing his/her signature below:

_____ _____
Name of Person Signing Date

_____ _____
Signature Telephone

_____ _____
Title Email