ALASKA RAILROAD CORPORATION
327 W. Ship Creek Ave.
Anchorage, AK 99501
Phone 907-265-4467
Fax 907-265-2439
HopeM@akrr.com

July 26, 2021

Addendum Number 1
Informal Request for Proposal 21-IRFP-209100
ARRC IT Security Assessment Services

This addendum is being issued to provide information as follows:

1. Proposal Due date is extended to 3:00 pm, August 16, 2021.

Questions/Answers:

2. **Q:** Will the Vendor performing this work be allowed to bid on the remediation work?

A: Yes.

3. **Q:** What is the size of the business environment?

a. How many employees do you have?

b. What are your mission critical applications? (web based, COTS, and bespoke/inhouse)

c. How many end-point devices do you have (PCs, tablets, laptops, etc.)**?**

A:

a. The Alaska Railroad has about 700 employees during peak times, and will have about 600 employees during 'off season'.
b.

1. Active Directory based systems.
2. We use IBMi for our Container and billing management systems, asset management and accounting systems
3. Microsoft desktop application stack
4. Developed and COTS code is used across the organization.

Further discussion of this will need to be in confidence for security reasons.

c. We have approximately 750 PCs, 50 tablets, 150 laptops, 500 servers, and 200 networking devices that will be in scope for this assessment.

4. **Q:** What is the size of your on-prem and cloud environment? (Quantity, how many servers, network environments, internal subnets, DMZ-subnets, etc.)

A: On-Prem (99% of environments)

- Approximately 500 servers
- 1 primary corporate environment
- 2 Operations Environments
- Most databases have at least Test and Production with many having Development as well
- We use approximately 50 /24 subnets
- We have 2 DMZ subnets

Cloud (limited)

- Only a few services/pieces of software operate in the cloud
- **Other than the social engineering email component, ARRC is limiting the scope of this assessment solely to on-premise services and systems.**

5. **Q:** How much operational technology do you want the vendor to get involved with regard to NIST SP 800-82 Industrial Controls??

   A: Our NIST SP 800-82 networks are, in some measure, tightly controlled and well understood. Traffic is monitored carefully and policies are more restrictive for what can connect and how. The operations network is also vast and some of the segments may carry some unknown risk. We would like to highlight 4 areas for testing. These will be:

   - An example Test Database/App/Presentation/PC
   - An example Train/Locomotive Stack
   - An example Wayside Device Stack
   - An example Communications Stack

   We will also want to walk many of the subnets present for our Operations subnets, and determine the devices that are on them, and make a determination as to what to test/penetrate.

   You can expect approximately 25% of this project will be used in determining risk from our operations networks/devices/and software.

6. **Q:** How are the geographically widespread environment connected to each other?

   A: The Alaska Railroad has offices in Seattle, and from Seward to Anchorage to Fairbanks. We have dozens of remote locations that are reachable by our network. Over 50 wayside locations (with network and power), along with major operations centers in 2 cities, and less significant operation centers in 6 others. We are connected via fiber between most of our locations, but also use radio transmission north of Anchorage. More discussion of this will need to wait until the award.

7. **Q:** What is your top Security person's title and who does that person report to?

A: Glen Biegel, CISSP, is the Manager - Service Delivery and Security, Technology. He reports to the Director, Technology.

8. **Q:** If we rely on sampling due to size, could you provide an example of your best baseline standardized environment/facility?

   A: There are Six Independent Areas of Concern that will come together in this Cybersecurity Assessment.

   1. Communications
   2. Operations Waysides
   3. Northern and remote stations
   4. Primary Corporate Network
   5. Train Operations Test
   6. Train Operations Production

   In each of these areas, there will be between 1 – 10 sample systems can be identified that can be considered a baseline set, and will need to be assessed and aggregated specifically along with the broader enumeration and identification tools. It is expected that critical risks will be identified broadly with an administrative level authenticated scan to give ARRC a complete picture of our risks and vulnerabilities. More specific discussion of baseline systems will have to wait until an award is made.

9. **Q:** Will all vendor questions be posted with Q&A?

   A: Yes, all vendor questions will be answered via addendum to the project.

10. **Q:** Do you have facilities that require a security clearance for entrance?

    A: Yes. Nearly all Railroad facilities have restricted access and limits on who can be present. All track areas have federal restrictions as well as to who can be present.

11. **Q:** Is the awarded Vendor required to have a business license??

    A: Per AS 43.70.020(a) a business license is required for the privilege of engaging in a business in the State of Alaska. Department of Commerce, Division of Licensing is responsible for business license mandates. For more information, or to determine whether an Alaskan Business License is required for your firm, please visit their website or contact them. https://www.commerce.alaska.gov/web/cbpl/BusinessLicensing.aspx
    Further clarified in ARRC Procurement Rules, 1300.2 Request for Proposals (e) If the offeror maintains an office or place of business in Alaska, the offeror must have a valid Alaska business license at the time designated in the request for proposals, for opening of the proposals.

12. **Q:** Is ARRC funded with federal funds?

    A: ARRC does use Federal funds as well as other funds for other operational or project related services. However, this project is funded with internal Capital funds.

13. **Q:** Given the broad nature and complexity of the ARRC's project for these critical security assessment services, we request ARRC consider extending the deadline to August 16, 2021. This extension benefits ARRC by allowing all vendors who have external security expertise and proven past performance an effective amount of time to develop a cost-conscious, comprehensive responses. It makes best use of ARRC project resources and sets the foundation for successful implementation and service delivery.

    A: The proposal deadline has been extended to August 16, 2021.

14. **Q:** [Task 1] The RFP states that there are approximately 1,700 systems in-scope. How are these split between internal and external?

    A: All are internal.

15. **Q:** [Task 1] The RFP refers to web application tests. How many web applications are in-scope?

    A: Five web applications are in scope.

16. **Q:** [Task 2] How many emails/phone numbers are in-scope?

    A: Fifty emails/phone numbers are in scope.

17. **Q:** [Task 3] How many locations are in-scope? How many wireless networks does each location have?

    A: Three locations, all on the same wireless network, with multiple access points.

18. **Q:** Is a SCADA system involved in this engagement, if so, what percentage of the overall testing will require SCADA specialized penetration testing?

    A: See response to question 5.

19. **Q:** Do you want a Quantitative NIST/CSF information security assessment completed as part of this engagement, which will also produce a risk score and maturity level score? If so, which task item would you like that included in for costing purposes?

A: NIST/CSF expertise is strongly desired for this assessment. While a full Quantitative assessment is beyond the scope of this IRFP, a sampling of related systems resulting in an estimated NIST/CSF risk/vulnerability score and mitigation strategies are within scope.

20. Q: In respect to page 17 / Minimum qualifications (f) does the proposer need to authorized to perform work in State of Alaska prior to submitting response or, can vendor provide prior to award once selected as vendor of choice? In other words, True North Consulting Group will provide this documentation if selected as vendor of choice. No issues with this requirement. TNCG conducts business nationally in Cybersecurity Consulting going on 37 years. We've got many / many certificates of good standing with states as well as certificates to conduct business. Not currently with Alaska. If we are required to receive authorization to conduct business in Alaska for this assessment, it will be done. In other words, if shortlisted as a vendor, authorization will be applied for and approved prior to contract execution if selected vendor of choice. From date of application, what's the time frame for approval?

A: See response to question 11.

21. Q: Task 3 Wireless Assessment, Pg. 10 Wireless Site Surveys. How many sites and devices will need to be surveyed? If there are multiple sites, what are their locations? What is the timeline for these surveys to be completed?

A: See response to question 3. Timeline for surveys will be established during negotiations.

22. Q: Task 6 Internal Administrator-level Authenticated Vulnerability Scan Pg.12

a. Does Alaska Railroad want a full scope assessment compared to the standards PCI-DSS, HIPPA, NIST SP800-53/82, ISO 27002 or review of the technical scope areas against those standards?
b. Does the organization intend that the auditor will review written documents and interview staff to complete the reviews according to the standards?

A:

a. ARRC has self-certified the areas of our network that require HIPAA, PCI-DSS, NIST SP800-53/82. Our goal is not to provide a full security assessment in any of these realms, but to validate our current security posture, or to provide mitigations for found to be deficient.
b. We will not have an auditor review the written documents in the sense of providing ARRC with a certified external audit report for PCI-DSS or any other standards. These documents are for ARRC's understanding of the success/status of our cybersecurity mitigation measures.

23. Q: Task 1 Technical Security Assessment. What is the number of IP's within your organization? How many are internal vs, external. Additionally, how many of the IP addresses are live?

A: See response to questions 3 and 4. Additionally, you asked about how many IP's are active within the organization. Some routing devices carry many IPs, as do some systems. There are approximately 4000 IPs that are present within ARRCs networks. Some of these will be designated out-of-scope, and many other areas will be assigned a sample for assessment, rather than have a network-wide scan.

24. Q: Is it the preference of Alaska Railway to use a local vendor to limit any travel costs?

A: Many, if not all, of these tasks can be done remotely or with minimal on-site activity. There is no preconceived notion on the extent of travel costs for the project or preference for Alaska Vendors.

25. Q: Task 4 Database Assessment. Which database systems are included in the scope of the database assessment? i.e. Microsoft SQL, Oracle, MySQL, etc?

A: IBMi/DB400, Microsoft SQL are included in the scope of the database assessment.

26. Q: Task 2 Social Engineering (Phone and E-Mail)

a. How many employees do you want to have the phone and e-mail social engineering efforts applied to? We recommend a minimum of 50.
b. Page 10 Physical Access—please clarify if onsite social engineering is within scope. If it is in scope, how many sites are to be tested? What are their locations and the timeframe required for testing?

A:

a. See response to question 16.
b. Onsite social engineering/penetration testing is within scope. Part of this assessment is to determine the relative security risk of our physical facilities (both office and operations), as well as our communications infrastructure. A minimum of 2 sites with personnel should be tested and at least one wayside site. The testing sites will be Anchorage and one additional site within 100 miles of Anchorage. Timeframe for testing is up to the vendor, but suggested in the September/November timeframe based on our award schedule.

27. Q: Web Application Security Testing The following set of questions are regarding, Task 1 (Technical Security Assessment) on page#5, Task 4 (Database Assessment) on page#10, and Task 5 (Brute Force Attack (Dictionary Attack)) on page#11 of the RFP document.

a. What kind of business-related services do your applications cater to?
b. The application referred to in the RFP document are in production or pre-production?
c. What is the objective behind this security testing? example: Any security failure in recent time, Audit, Compliance, etc. (Example: PCI HIPAA, NIST)

d. Please specify the total number of Applications in scope?
e. Please specify if any payment gateways are to be considered as part of the scope? If yes, please provide related details.
f. How many different user roles are there within each application in the scope of the RFP? (What is their hierarchy?) Does our solution need to cover different user roles? (Ex: Super admin, Admin, normal user, Guest, etc.)
g. Please provide the architecture diagram of all the applications and networks under the scope of the RFP. (Application flow diagram with controllers, Firewalls, etc.)
h. Was the application in the scope of the RFP tested before? If yes, when was it last tested? Any specific concerns that we should know from the last test run? Please detail.
i. Do you have any specific requirements that are not covered in this document? please explain in detail if any

A:

a. This will be discussed at a later point. Other questions pertain to this, and you can visit AlaskaRailroad.com to view our public site.
b. During the discussion of the rules of engagement, as a team, we may elect to test either production or test/dev systems depending on their applicability and resilience.
c. Answered in other questions.
d. We will identify 5 applications in scope.
e. No payment gateways are in scope.
f. As required, we will identify 3 users/roles in each application to assist with drawing a boundary around/limiting the eventual scope of application testing.
g. This is not possible in this forum. Everything you need will be provided after a contract is established between the vendor and ARRC.
h. Our applications are patched regularly, but only penetration tested sparingly. You can consider the applications you will be reviewing as newly tested.
i. We will establish any other needed specifics after an agreement has been made to proceed with the vendor.

28. **Q:** External Network Security Assessment the following set of questions are regarding**, Task 3 (**Wireless Assessment**)** on **page#10** and **Task 6 (**Internal Administrator-level Authenticated Vulnerability Scan**)** on **page#12** of the RFP document.
    a. What is the objective behind this network and infrastructure security testing? Example: Audit, Compliance, etc.
    b. Please provide a network architecture diagram
    c. Does your team have any specific preference regarding where the engagement is to be executed?
    Onsite, Offsite, Both

d. Was the network tested before? If yes, when was it last tested? Any specific concerns that we should know from the last test run? Please detail.

A:

a. Discovery of cybersecurity flaws and vulnerabilities. Areas where we believe we understand the risk of devices, but do not.
b. This will be provided when we finalize the contract.
c. We have no preference. We expect that the vast majority of effort will be offsite, and that some of the tasks will require a physical presence.
d. Yes, the network is tested periodically. This is not information that can be shared outside of a contractor relationship.

29. Q: Social Engineering Assessment. The following set of questions are regarding, Task 2.

a. How many server types are used in your network? Please respond in detail.
b. How many device types are used in your network? Please respond in detail.
c. Do you have any specific requirements that are not covered in this document, please specify if any.

A:

a.

Application Server	~50
Web Server	~10
Proxy Server	2
Authentication Server	~10
Mail Server	~6
Database Server	~10

Others (Please Specify) There are a total of approximately 500 servers in the architecture.

b. Switches, Routers, Firewalls, Gateways: There are approximately 200 network devices that will be in scope of various types in this engagement.
c. We will make a final agreement after the award has been made. For security and other reasons, the full scope and specifics can't be provided in these communications. Any specific requirements will be agreed to by both parties and included in a fixed final contract.

30. Q: Social Engineering Assessment. The following set of questions are regarding, Task 2 (Social Engineering (Phone and E-mail)) on page#9 of the RFP document.

a. What kind of assessment you are looking for? Example: Red teaming or standalone or any other type (please specify).
b. If standalone - Please specify the number of employees, Help desks.

A:

a. For the Social engineering phase, approximately 50 emails and/or phone numbers will be provided for testing purposes. The vendor may elect to perform the social engineering.
b. Same answer as a.

31. Q: Various Questions

a. RFP Page 16 requires a 20-page response limit, including "exhibits." Does this include the required response forms (RFQ pages 22-29)?
    - Are methodologies for the work to be performed also to be part of the 20-page count or can they be submitted in an appendix?
b. Have these services been performed before for ARC, and if so, how recently?
    - If previously performed:
        - Who is the incumbent?
        - Are they allowed to bid?
        - What was the contract value of the last project?
c. Regarding RFP pgs. 7-8 web application review, how many web applications are in scope?

A:

a. The 20-page response limit does not include the 2-page introduction letter, the questionnaire, or resumes; however, all other items are included within the page limit.
b. We have had a major assessment in 2016, and minor assessments since then. We are unable to provide the previous assessor's name, but they are entitled to propose. They have not been consulted or contacted during the development of this assessment IRFP. The previous contract value was approximately $70K.
c. See answer to question 28.

32. Q: Is it possible to get pages 22-29 in editable format for filling in text?

A: Section F is best edited using Adobe, ARRC does not have the document in a format that would otherwise be easy to fill. A hand-written response is acceptable.

33. Q: How many networks (subnets) are in the infrastructure to be included in the segmentation testing?

A:
IBMi/DB400 - 6 instances of the database will need to be assessed.
MS SQL 6 instances and 15 databases will need to be assessed.

34. Q: How many SSIDs are included in the wireless network?

A: There is one SSID included in the wireless network.

35. **Q:** Can you share your budget for this project?

    A: The initial cost is estimated to be in the range of $55,000 to $62,000.

36. **Q:** Do you have an anticipated project schedule or deadline that the work must be completed by?

    A: It is the desire of the ARRC that all work within the scope be completed by December 31, 2021.

37. **Q:** Due to the confidential nature of our security business as well as existing NDAs, we would like to provide anonymized references at this RFP stage, i.e., we would provide project implementation details, but the client would be described, not named, and specific contact information would be withheld for now. Reference calls would be coordinated upon request at down-select. Would this approach be acceptable to the Alaska Railroad Corp for this RFP response?

    A: Yes, that is acceptable; however, it may adversely influence the evaluation of your firm if enough information cannot be derived from what is provided. Any information deemed to be confidential in nature may be proposed as such. The Contracting Officer will consider all requests to keep information confidential on a case by case basis.

All other dates, terms, and conditions remain unchanged.

The above are all of the questions we have received to-date. If you have already submitted your questions and they were not answered herein, please contact the Contract Administrator.

Acknowledge receipt of this and all addenda on your firm's Service Bid Form (Form 395-0132). Failure to acknowledge addenda may be cause for rejection of your proposal. It is the Offeror's responsibility to assure they have received all addenda for the project.

Sincerely,

Michele Hope

Michele Hope
Contract Administrator
Alaska Railroad Corporation