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

August 10, 2021

Addendum Number 2
Informal Request for Proposal 21-IRFP-209100
ARRC IT Security Assessment Services

This addendum is being issued to provide information as follows:

Questions/Answers:

1. **Q:** How many internet (publicly) routable IPs are in scope for the external network/host penetration test?

   A: Approximately 12 servers, and 4 devices.

2. **Q:** Do you have IDS/IPS in place? If so, does it actively deny/block suspected attacks?

   A: We have both IDS and IPS in place. Yes, it can/does block attacks.

3. **Q:** Do you have a Web Application Firewall in place?

   A: We have a proxy and port restrictions, but not a full WAF in place for our externally accessible sites.

4. **Q:** Do you have any other perimeter security controls in place that we should be aware of (i.e. white-listing, etc.)?

   A: There are external controls, but these will have to be discussed after an agreement and NDA is in place.

5. **Q:** Please provide the list of external IPs that are in scope for testing.

   A: Our external IP address space is publicly available, but the specifics will have to be discussed after an agreement and NDA is in place.

6. **Q:** How many networks comprise your internal corporate/enterprise infrastructure?

   A: Previously answered in Addendum 1.

7. **Q:** How many RFC 1918 (internal) IP addressable devices exist across your corporate/enterprise LAN infrastructure?

A: Previously answered in Addendum 1.

8. **Q:** Please provide the IP addresses or ranges in your LAN data networks. (Note, this can be provided later during the chartering process in the ROE.)

   A: Previously answered and will be provided after an agreement and NDA is in place.

9. **Q:** Do you isolate your most sensitive data in segmented networks? If so, how many LAN segments exist?

   A: Yes. We do, and this will be discussed after an agreement and NDA is in place.

10. **Q:** How many RFC 1918 (internal) IP addressable devices comprise your sensitive data networks?

    A: Approximately 20 subnets are designated as sensitive.

11. **Q:** Please provide the IP addresses or ranges in your sensitive data networks. (Note, this can be provided later during the chartering process in the ROE.)

    A: This will be discussed after an agreement and NDA is in place.

12. **Q:** How many different types of segmentation technologies are used to implement network segmentation which isolates your sensitive data networks from your standard (open) user networks?

    A: Approximately 4, depending on your definition.

13. **Q:** Can testing of the internal network be performed via remote connectivity or can testing be done using a device (aka “drone”) sent to the location? In lieu of remote or “drone”, will our staff have to be onsite at your location to perform testing?

    A: Yes, drone testing will be supported.

14. **Q:** Can all testing of the internal network components be done from a single network location? Or will travel to multiple locations be required? If so, please identify the number and locations.

    A: We may need to connect the testing device to separate networks depending on the ROE, and agreement between internal teams.

15. **Q:** How many Custom Web Applications are in the external network?

    A: Very few, mostly including APIs. AlaskaRailroad.com can be considered a custom web application.

16. **Q:** Do these applications require credentials or some type of personally identifying data to access application functionality?

A: In all cases yes, except the AlaskaRailroad.com website.

17. **Q:** If yes above, how many different roles are supported by the application? Please identify the role and type of access achieved by an authenticated user of that role.

    A: There are 5 web based applications that are expected to pen tested. This will include 2-3 externally accessible applications.

18. **Q:** Will application testing be done in the production environment or in a test/staging environment? Application testing can be done in test/staging if the code instance in this environment is a duplicate of the code in production.

    A: ARRC expects most testing to be done in our test/staging environments. Some production pen testing may be selected.

19. **Q:** Do you have an active Web Application Firewall (WAF) in place?

    A: No.

20. **Q:** For custom web applications, are you looking to have a static code analysis done on the source of the application?

    A: We look to our assessors for recommendations on this. It may be more productive to work the pen test from the front end or the programmer side.

21. **Q:** If applicable, what language/framework is the application developed in?

    A: We have a few, but they are well known and will have to be discussed later in the process.

22. **Q:** If applicable, how many lines of code (LOC) are in scope for the code review?

    A: To be negotiated once contract is awarded and dependent on skill sets and approach to the services.

23. **Q:** Are any facilities in scope for wireless testing?

    A: We are looking for 2 facilities to be reviewed.

24. **Q:** Please provide address(es) for all facilities that are in scope for wireless testing.

    A: These are in Anchorage.

25. **Q:** Is social engineering in scope for this project?

    A: Previously answered in Addendum 1.

26. **Q:** For phishing attacks, how many targets are in scope for this project? Or, in lieu of a specific number of targets, what percentage of the employee population is to be targeted?

A: Previously answered in Addendum 1.

27. **Q:** For pretext calling attacks, how many targets are in scope for this project? Or, in lieu of a specific number of targets, what percentage of the employee population is to be targeted?

A: Previously answered in Addendum 1.

28. **Q:** Will you provide the target details (i.e. names, email addresses, phone numbers, etc.) or are you looking have this information discovered through reconnaissance of publically available information?

A: If you can demonstrate what information you can obtain for a single target through public sources, then ARRC will provide that same level of information for all of the targets.

29. **Q:** How many facilities are in scope for physical social engineering (tailgating, impersonation, etc)?

A: Previously answered in Addendum 1.

30. **Q:** Please provide the address(es) of all facilities in scope for physical social engineering.

A: All are within Anchorage.

31. **Q:** Can all testing be performed during "normal" business hours (6am Eastern - 6pm Pacific Monday – Friday)?

A: Yes.

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. Please assure your questions have not already been answered before submitting.

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