RAILBELT RELIABILITY COUNCIL

REQUEST FOR PROPOSALS: IT SPECIALIST

RAILBELT RELIABILITY COUNCIL – REQUEST FOR PROPOSALS (RFP)	DATE LISTED: 1/26/2024
RFP TITLE: SYSTEMS ARCHITECTURE/SECURITY ENGINEER ADVISOR	SUBMISSION DEADLINE: 3/1/2024
RFP NUMBER: 20240126-01	ANTICIPATED START DATE: 3/20/2024

1. INTRODUCTION

The Railbelt Reliability Council (RRC) is seeking a talented and experienced Systems Architect/Security Engineer who can advise the RRC on the IT system architecture necessary for a document management system and advise on the systems needed to integrate that document management system with the RRC's public website. The Infrastructure Committee of the RRC (InfraCom) will ultimately select a firm based on the firm's understanding of the needs of the RRC, the qualifications of the proposer, and other elements included in Section 4 of this document.

2. BACKGROUND

The RRC is an Electric Reliability Organization (ERO) that is responsible for developing operating and reliability, critical infrastructure protection, cybersecurity, and open access standards as well as leading open public processes to develop regional integrated resource and transmission expansion plans for the Railbelt, the largest interconnected bulk electric system in Alaska. As a not-for-profit organization with a statutory mandate to provide public information and allow for public participation in work product development, including standards and plans, the RRC has developed a structured approach to work product development.

Work products will be developed in working groups consisting of technical experts and stakeholder representatives. Technical experts, either RRC staff or consultants, will develop and iterate on documents within an internal document management system, and then bring these materials to public working group meetings. To comply with regulatory requirements, all materials presented to the working groups will need to be made publicly available through the RRC's website. Other administrative documents will also need to be generated from internal staff and/or consultants and posted to the website, such as RRC Board and Committee meeting materials, proposed budgets and associated documents, and other miscellaneous documents. Internal documents used to formulate the public material will need to be revision controlled and stored, but will not be made available through the RRC website.

The RRC expects to hire engineering staff in mid-2024, and in order for them to be able to begin effective work in a timely manner, the IT infrastructure for managing and controlling documents must be outlined at an architectural level. All RRC documents must be housed and maintained in the internal document management system, while select documents will be published to the website in the most automated manner possible while maintaining the highest level of security possible both within the RRC

internal document control system and the public-facing website. In addition, certain public comments, but not all, may be submitted to the RRC through the website interface. These comments will be pushed to the internal document control system for management and distribution.

There is an ongoing effort to upgrade the current RRC website, and while the focus of this ongoing effort is front-end improvements, there is an opportunity to make changes to the website which will streamline future integrations with the future document management system.

A document management system must be capable of the following features:

- Version control; there must be a formal process for updating documents and the system should automatically retain historic versions of documents which should be readily available to specified users.
- Access control; The system must have the ability to control access to certain documents, for instance, members of working groups may have the ability to edit certain documents whereas other RRC staff may have read-only or no access.
- Ability to post to the website securely; Ideally, internal documents should be able to be published on the website with a single action.
- Search; There should be an ability to search the website for documents based on document title, dates, authors, document content, and/or user-generated tags.
- Ability to search within the document management system with similar search parameters.
- Support; There must be the ability to troubleshoot issues through web searches, or other dedicated systems.
- Backup and system recovery; Must have a system for regularly backing up documents for recovery in the case of system failure, cyber-attack, or other unforeseen circumstances.
- Industry best practices for securely storing critical infrastructure security.
- Cost at scale; The system must be reasonably priced even when utilizing large amounts of data.

Currently, the RRC does not have sufficient Cybersecurity/Systems IT expertise to design the architecture of this integration or to ensure the current website upgrades will be compatible with future document control systems. An expert is needed to recommend systems that are designed securely and effectively.

3. Scope of Work

The Systems Architect/Security Engineer will be responsible for the following:

- Attend relevant RRC Committee meetings;
- Inform the RRC about document management systems available and interfaces to external sites;
- Advise the RRC on cybersecurity strategy for the document management system and website and integrations between the two systems, considering that the RRC documents may include critical infrastructure material subject to security standards of the Railbelt Load Serving Entities;
- Design and provide systems architecture diagrams and documents based on industry practice and knowledge of industry practices and fundamental principles, as well as RRC input;
- Advise the RRC on physical and virtual infrastructure solutions necessary to implement the desired system architecture; and

- Coordinate with web designer and administrative consultants and/or staff to ensure system architecture is compatible with website.

The scope of work will specifically not include the following:

- Implementation of the document management system;
- Choosing a document management system; or
- Implementation of systems for the integration of the document management system and website.

4. Selection Criteria

The following criteria will be considered for selection:

- IT Systems architecture expertise;
- Cybersecurity expertise;
- Experience with critical infrastructure cybersecurity; and
- Experience integrating document management systems for engineering applications.

5. Bid Selection Schedule

The RRC will make all reasonable efforts to adhere to the bid schedule below but reserves the right to amend key dates listed as required. Changes to the schedule will be communicated to bidders as deemed appropriate.

Event Description	Date and Time (Alaska Time)
Date Listed	1/26/2023
Questions Due	2/16/2024
Proposals Due	3/1/2024
Anticipated Decision Date	3/6/2024

6. RFP Instructions & Rules

6.1 Instructions for Submitting a Proposal

Proposals should be submitted to info@akrrc.org. Infrastructure Committee Chair Greg Stiegel (gstiegel@realaska.org) should be copied to submissions.

Any questions regarding this RFP submitted to mmorehouse@sapereconsulting.com and the RRC administrative email account (info@akrrc.org) will be considered and any responses necessary will be made within two (2) business days.

6.2 Evaluation & Selection

Proposals will be evaluated on cybersecurity knowledge and experience, experience with document management systems, relevant experience with related organizations, and expertise of key staff.

7. SUBMITTAL ITEMS

- Signed Proposal Cover Page
- Documentation that the proposer either possesses a current Alaska Business License, maintains an office and staff within Alaska, is incorporated in Alaska, or is registered as a foreign corporation authorized to do business in Alaska;
- A proposal for one (1) month of Systems Architecture/Security Engineer advisory services including:
    - A description of the proposer's team including resumes of key member(s);
    - Verifiable experience and expertise within the electricity industry;
    - Verifiable experience and expertise with cybersecurity especially regarding critical infrastructure;
    - Verifiable experience and expertise with backend website architecture;
    - Verifiable experience and expertise in implementing document management systems;
    - Demonstrated comprehension of the RRC's required services and clearly articulated strategy for performance including: A description of activities to initiate services and develop recommendations;
    - Evidence of the proposer's capability to provide the requested scope of work and ability to integrate the proposed system; and
- Under a separate seal, a cost proposal detailing estimated personnel hours and billing rates. The RRC will consider cost proposals for services provided on a time and material basis.

PROPOSAL COVER PAGE

REQUEST FOR PROPOSALS: [INSERT RFP TITLE AND NUMBER]

SUBMITTAL INFORMATION	
Submit this completed form as the cover page of your proposal	
DESCRIPTION	
Request for Proposals (RFP): [Insert RFP number]	[Insert RFP title]
OFFEROR INFORMATION (TO BE COMPLETED BY OFFEROR)	
BUSINESS INFORMATION _____ Company/Organization Name _____ Address _(_____)_____ Telephone number _____ Website Address _(_____)_____ Fax Number (optional)	**REPRESENTATIVE AUTHORIZED TO SIGN OFFER** _____ Authorized Representative (AR) Name _____ AR Title _____ AR Email Address _(_____)_____ AR Telephone Number _____ AR Mailing Address
SIGNATURE	
I certify that all RFP instructions, rules, explanations, and scope of work have been reviewed, understood, and complied with; and that all information in this submission is true, correct, and in compliance with the terms of the RFP. _____ Authorized Representative Signature _____ Date	