Oregon TECH
Procurement & Contract Services

Klamath Falls:
541.885.1133 (office)
3201 Campus Drive
Klamath Falls, OR 97601

Portland-Metro
503.821.1266 (office)
27500 SW Parkway Avenue
Wilsonville, OR 97070

REQUEST FOR QUOTES #2024-03
NIST COMPLIANCE IMPLEMENTATION
RESPONSE TO CLARIFYING QUESTIONS II
March 5, 2024

Note that these are questions submitted by interested firms to this solicitation. The below answers are for clarification purposes only and in no way alter or amend the RFQ as published.

1. RFQ states: "Data is stored in a combination of cloud-based environments supported by Oregon Tech and local on-site servers maintained by the MSP."

    a. QUESTION: Does OMIC have a documented inventory of systems and information, and know where CUI exists today?

    ANSWER: Currently we do not, however, will need to in the future. There will also need to be involvement of Oregon Tech Office of Sponsored Research regarding future contracts.

2. RFQ states: "The OMIC campus contains two (2) physical buildings that house over fifteen (15) employees and technology/network hardware."

    a. QUESTION: Is the scope within the entire college, including the 15 employees? Will students have access to CUI (what is the expected total number of users expected to have access to CUI)?'

    ANSWER: The scope is with OMIC R&D and not all of Oregon Tech. It is anticipated that not all of the 15 employees will need full time access to CUI that is housed for specific R&D projects. Students, unless actively working with OMIC as interns or research assistants would not have access to any CUI.

    b. QUESTION: Are there opportunities to reduce the number of servers/storage devices in which CUI resides (i.e., is a re-architecture to create a CUI 'enclave' under consideration and/or part of the scope)?

    ANSWER: Based on the assessment and recommendations as the controls are implemented, OMIC is open to setting up a secure environment in conjunction with OMIC's MSP partner.

3. RFQ scope (lettered items) includes: "Help determine tasks/projects to be completed by Fractional CIO/MSP post assessment."

    a. QUESTION: Is this in reference to defining post gap assessment remediation tasks and projects?

ANSWER: Yes, these are Post Assessment tasks in order to meet the standards of the NIST 800-171 controls.

b. QUESTION: To what level of detail are these tasks/projects to go – a listing of items with brief descriptors, or formal project plans with scope, timeline, Gantt chart etc.?

   ANSWER: Includes creating an understanding of the Control in question, detailing from the assessment why it is not met and suggestions for remediation in order to meet the control.

4. Letter C. States: "Develop policies, procedures, and controls in accordance with NIST guidelines (implementation will be handled by Fractional CIO and MSP)."

   a. QUESTION: Can that be interpreted as 'develop all CMMC required documentation,' or is the scope purposely limited to Policies, Processes, and controls (should the vendor include creation of SSP, POA&Ms, etc.)?

      ANSWER: Any policies, processes, and procedures necessary to meet and adhere to the NIST controls.

   b. QUESTION: To confirm - no oversight or assistance with implementation of controls is in scope?

      ANSWER: No assistance is required with the implementation of the controls. Review of what was done will be necessary to have joint understanding and agreement that the control is met.

   c. QUESTION: Is implementation of, or use of existing 'Risk Management' or Compliance Management software/platform, in scope?

      ANSWER: If this is the preferred method of tracking of the contractor, it can be suggested for use.

5. QUESTION: Is there an existing security program in place?

   ANSWER: There is no existing security program in place. This is new ground for OMIC R&D, as we are hosted by Oregon Tech with specific needs and requirements.

6. QUESTION: Are there existing documented policies and procedures?

   ANSWER: There are no existing policies as this is a new initiative of OMIC R&D.

7. QUESTION: Is there an Incident Response Plan in place, or is development of one in scope?

   ANSWER: OMIC does not have its own Incident Response Plan, but it does adhere to the procedures of Oregon Tech which maintains control of OMIC's MS365 environment.

8. QUESTION: Is there a security event and incident monitoring system in place? A security operations center or other security incident response capability?

   ANSWER: No, there is not.

End of Clarifying Questions II