Roanoke Regional Airport Commission
RFP # 23-011
MANAGED CYBERSECURITY SERVICES
Addendum #3
June 7, 2023

The contents of this addendum represent solicitation questions and answers, notes, changes, additions or clarifications to the specifications. A conformed copy of the RFP reflecting all changes from Addendum #3 is also included as a separate attachment if needed.

Questions and Answers – RRAC RFP #23-011 – Managed Cybersecurity Services

Q1. **How many IT staff members does RRAC have?**

A1. We have one IT manager and a planning director over the manager.

Q2. **Would RRAC accept a SIEM solution delivered by a Security Operations Centre located in Canada?**

A2. Yes, we would gladly accept a SIEM solution delivered by a vendor located in Canada as long as TSA & FAA see no issues with it.

Q3. **Please clarify, "The RRAC will maintain operational control of all existing security appliances and systems." Is this to mean Roanoke will maintain day to day operations and are only looking for advice on policy/security controls?**

A3. Commission staff will maintain operational control of existing security appliances and controls. The respondent will be expected to provide expertise regarding cybersecurity vulnerability assessment, mitigation, and compliance.

Q4. **Can Roanoke provide a copy of the TSA directive to help verify pricing and scope of work?**

A4. RRAC can only provide a copy of this directive to the selected vendor

Q5. **Can you confirm that the Addendum #2 "III. Scope of Work Clarifications" is replacing the "Scope of Services" and "Deliverables Required" from the original RFP?**

A5. Addendum #2 is intended to clarify items 4, 5, and 6 of the scope on the original RFP. Everything else from the original RFP should be considered unchanged.

Q6. **The vendor requirements that were in the original RFP are not present in the new Scope of Work. Are these still requirements?**

A6. See A5 above.

Q7. **What will be the term of this contract or is it an open-ended contract?**

A7. The term will be for one year initially with the option to renew for four (4) additional one-year terms.

Q8. **Would the Commission entertain adding a cooperative procurement clause to this contract?**

A8. Yes.

Q9. **With respect to pricing, is there a certain format that you would like for everyone to use? Also, how would you like for us to address pricing for services where detailed scoping calls are required?**

A9. Annual pricing, with additional hourly rate as needed.

Q10. **Does RRAC intend to utilize Watchguard as its EPDR technology? If not, would RRAC be open to any of the technologies listed below:**

1. **Microsoft Defender for Endpoint**
2. **Palo Alto Cortex XDR**
3. **Crowdstrike**
4. **SentinelOne**

A10. Yes, there is no intent to move away from existing appliances or controls.

Q11. **Does RRAC intend to utilize Watchguard as its firewall technology? If not, would RRAC be open to any of the technologies listed below:**

1. **Cisco**
2. **Fortinet**
3. **Palo Alto**
4. **Checkpoint**

A11. See A10 above.

Q12. **Are there detailed functionality requirements of the SIEM service referenced in this RFP that can be provided? Specifically, does it need to support any/all of the requirements below?**

1. **Custom log source ingestion**
2. **Operational IT use outside of a security focus**
3. **SOAR capabilities**

A12. The respondent is expected to provide options to support all three.

Q13. **If yes to any of the three requirements above, please elaborate as the details of each.**

A13. N/A

Q14. **Would it be acceptable to the awarded vendor to partner with a third party to provide IT cybersecurity solutions?**

A14. No.

Q15. **Will you please categorize the IT and OT assets for the all of the line items listed in the addendum?**

A15. OT assets are not included in the scope.

Q16. **Please explain what control and oversight of the IT and OT assets you expect? (Are you expecting the vendor to recover failed devices?)**

A16. We expect continuous monitoring and analysis of security events, as well as timely identification, containment, and mitigation of incidents.

Q17. **Page 2, items 1 and 2 appear to be in conflict - The requirement for 24/7/365 Monitoring and Incident Response and then Item 2. says the RRAC will maintain operational control of all existing security appliances and systems.**

a) **Could you please elaborate on what actions, if any, you allow your service provider to perform in making an incident response for containment, mitigation, and node/system recovery?**
b) **Are you expecting the Service Provider to provide alerts to your personnel and your personnel take all actions?**
c) **Or are you expecting the Service Provider to take actions on the system?**

A17. See A3 and A16. RRAC staff will make the final decisions on and will perform any system changes that are required.

Q18. **Do you have a Security Operations Center (SOC) that will operate/ utilize the SIEM on-site? If so, could you please characterize what would be integrated with the SIEM?**

A18. No. The respondent will be expected to operate the SIEM solution, although Commission staff will also need to have access to the platform along with any appropriate user training.

Q19. **If the selected vendor offers an OT SIEM, may that vendor partner with a third party to connect the IT SIEM?**

A19. See A15.

Q20. **Should a vendor focus on the RFP scope, which encompasses the provision of comprehensive cybersecurity services? Or should we incorporate the requirements outlined in Addendum 2 and include the provision of a SIEM software solution?**

A20. The intent of Addendum #2 was to clarify our needs in a SIEM solution and trump the original RFP.

Q21. **If a firm does not have direct experience with an airport, would that disqualify us from the bid?**

A21. No, it would not disqualify them if relevant experience can be shown

End of Addendum #3