Roanoke Regional Airport Commission
RFP # 23-011
MANAGED CYBERSECURITY SERVICES

Addendum #2
May 25, 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 #2 is also included as a separate attachment if needed.

I. Proposal Due Date:

The proposal due date is hereby changed from June 2, 2023 at 3:00 p.m. to **June 14, 2023 at 3:00 p.m.**

II. Environment Outlook:

LDAP Environment: Microsoft Active Directory on-premises

Number of domain controllers: 2

Number of users: 60

Number of computers: 75

Number of physical servers: 4

Virtual environment: VMware ESXi, 2 hosts, 1 SAN on-premises

Number of virtual servers: 12

Backup environment: Veeam, on-premises storage

Wireless Controller: Watchguard Cloud

Number of access points: 25

Firewall: Watchguard M390 HA Cluster on-premises appliance

Endpoint security: Watchguard EPDR

Internet connection: 100 Mbps fiber optic

Public IPs: 6

Number of network switches: 22

Email environment: Microsoft Exchange Server on-premises

Number of mailboxes: 100

Spam filtering/antimalware: Fortimail on-premises appliance

Remote access: SSL-VPN with MFA

III. Scope of Work Clarifications:

The Roanoke Regional Airport Commission (RRAC) is currently seeking a comprehensive Security Information and Event Management (SIEM) software solution for the Roanoke-Blacksburg Regional Airport. The RRAC is responsible for ensuring the safety and security of the airport and its infrastructure, and we recognize the critical role that a robust SIEM solution plays in our cybersecurity strategy.

We invite your organization to submit a proposal for the provision of a SIEM software solution that meets the following requirements:

1. 24/7/365 Monitoring and Incident Response:

- The solution must provide continuous monitoring and analysis of security events, leveraging real-time threat intelligence and advanced analytics.

- The respondent must guarantee 24/7/365 monitoring capability and incident response to ensure timely identification, containment, and mitigation of security incidents.

2. Operational Control of Existing Security Appliances:

- The RRAC will maintain operational control of all existing security appliances and systems.

- The SIEM solution should seamlessly integrate with our current infrastructure and security tools, including firewalls, intrusion detection/prevention systems, and network devices.

3. Compliance with TSA Cybersecurity Directives, Department of Homeland Security initiatives and Commonwealth of Virginia Guidelines:

- The successful respondent must ensure compliance with all current and future Transportation Security Administration (TSA) cybersecurity directives and regulations, along with any applicable initiatives or guidelines from the Department of Homeland Security or the Commonwealth of Virginia applicable to the Roanoke-Blacksburg Regional Airport.

4. Cybersecurity Assessment and Remediation:

- The selected vendor must conduct a comprehensive cybersecurity assessment of the SIEM solution at least bi-annually.

- The assessment should encompass a thorough evaluation of the solution's infrastructure, configurations, and processes to identify any vulnerabilities or weaknesses.

- The vendor must provide a detailed report outlining the findings of the assessment, including identified vulnerabilities, associated risks, and recommended remediation measures.

- The recommended remediation measures should align with industry best practices and compliance requirements.

End of Addendum #2