REQUEST FOR PROPOSAL (RFP)
IT MANAGED SERVICES PROVIDER (MSP)

Introduction

The Metropolitan Airport Authority of Rock Island County, IL (MAA) is seeking proposals from qualified Managed IT Service Providers (MSPs) for comprehensive IT infrastructure, network security, and compliance services at the Quad Cities International Airport.

The MAA owns and operates over $240 million in assets on a 2,100-plus acre campus. Some of these assets include a 12-gate passenger terminal facility, a four-bay Fire/Police station, an airfield maintenance facility, rental car facility, cargo/airplane operation facilities, and other various buildings.

As a Transportation Security Administration (TSA) regulated facility, the MAA must comply with stringent cybersecurity measures to protect its Information Technology (IT) and Operational Technology (OT) systems. The selected provider must demonstrate a thorough understanding of TSA cybersecurity regulations including but not limited to:

- Continuous network security monitoring and segmentation
- Network and system access control with zero trust principles
- Regular patch management and vulnerability assessments
- Incident response plans and security awareness training
- Vendor risk management and supply chain security compliance

The MAA maintains an onsite IT Manager; therefore, while 24/7 help desk services are not required as part of the base proposal, they should be included at an hourly rate or as an addon to be available as necessary or as part of a critical incident response.

2. Scope Of Work

IT Infrastructure and Managed Services

1. **Infrastructure and Network management**

- On-Site SLA:
    - 2-hour response time (Monday-Friday, 6AM-6PM CST)
    - 4-hour response time outside normal business hours
- Server management, firewall management, network segmentation, and VPN administration
    - Can provide as managed service or per project
    - Provide monitoring and support hours

T: 309.764.9621
F: 309.757.1515

2200 69th Ave. Suite 100
Moline, Illinois 61265

QCairport.com

- Microsoft 365 and cloud security management and licensing

2. **Security Operations and Compliance**

- 24x7 cybersecurity monitoring and incident response
- US-based Security Operations Center (SOC) required
- Provider must have personnel located within the Quad Cities region to support on-site end user and infrastructure needs
- Vendors must detail their process for detecting and responding to threats that bypass standard Endpoint Detection and Response (EDR) tools
- The proposal must include a clear explanation of how the provider identifies, escalates, and neutralizes security threats in real-time.
- Vendor must outline their SLA for detecting and responding to cyber-attacks, including timeframes for containment and remediation.

3. **Backup and Disaster Recovery (BDR)**

- Cloud-based backups for Microsoft 365, endpoints, and servers
- Email security and archiving
- Immutable backups with ransomware resilience
- Fully tested server backups and disaster recovery plan
- Annual or full-scale disaster recovery test

4. **Privileged Access Management Software (PAM)**

- Centralized management of administrative access to server platforms with policy-based rotating administrative passwords and one-time account functionality.
- Rule based administrative rights elevation for end-user stations based on application and user request.
- Auditing of administrative access

Optional Add-On Services (Pricing must be provided separately)

- 24x7 Help Desk support for remote user assistance
- On-site hourly helpdesk for escalated issues
- On-site hourly network/server management for escalated issues
- Compliance audits and penetration testing
- Zero trust network access controls

T: 309.764.9621
F: 309.757.1515
2200 69th Ave. Suite 100
Moline, Illinois 61265
QCairport.com

Minimum Qualifications and Requirements

A. Vendor Experience

- Minimum 10+ years of experience in managed IT and Cybersecurity
- Must have a local office and support staff within the Quad Cities region
- Experience working with TSA, NIST 800-171, and CIS compliance frameworks
- Must provide US-based 24/7 Security Operations Center (SOC)
    - Defined SLA for responding to cyber-attacks, including:
        - Maximum time to detect an active breach
        - Time to respond and neutralize a confirmed security threat.
        - Process for providing incident reports and post-breach analysis.

B. Technical Requirements

- 24/7 cybersecurity monitoring and threat response
- Network segmentation, firewall management, and Zero Trust security policies
- Cloud, endpoint, and Microsoft 365 security services

C. Security and Compliance

- Must comply with TSA/CISA cybersecurity regulations and recommendations including:
    - Incident response planning and continuous monitoring
    - Patch management and vulnerability scanning
    - Multi-factor authentication (MFA) and least privilege control
- Vendor must carry a $5m Cyber Liability Insurance policy
- Vendor must list all third-party cybersecurity tools, software, vendors, and partners used.
    - This includes security monitoring tools, endpoint protection, SIEM, email filtering, backup solutions, and compliance tools.

D. Licensing

- Vendor must be a partner with Microsoft, and Cisco and be able to provide vendor-purchased licensing such as Microsoft 365 Business Standard (100 count), Cisco Duo (61 Count) and others. Listing of existing licensing and counts is available upon vendor request.

Proposal Requirements

A. Executive Summary

- Overview of the vendor's capabilities, approach, and experience.
- Summary of airport, transportation, or TSA/CISA-regulated experience

B. Technical Proposal

1. Infrastructure and On-Site Support Approach
    - Explanation of on-site support model and response SLAs
    - Infrastructure monitoring, automation, and patching strategies
2. 24/7 Cybersecurity Monitoring and Threat Response

T: 309.764.9621
F: 309.757.1515
2200 69th Ave. Suite 100
Moline, Illinois 61265
QCairport.com

- Detailed explanation of how the vendor detects and responds to threats that bypass EDR solutions.
- Specific escalation and containment process for active security incidents
- Explain testing process for Microsoft and 3rd party patches and SLA for deployment of zero-day vulnerabilities.
- Defined SLA for responding to cyberattacks, including:
    - Maximum time to detect an active breach.
    - Time to respond and neutralize a confirmed security threat.
    - Process for providing incident reports and post-breach analysis.

3. Cloud and Network Security
    - Approach to firewall, network segmentation, and VPN security.
    - Microsoft 365 and cloud access control best practices
4. Compliance and Vendor Risk Management
    - Strategy for maintaining TSA, NIST, and CISA compliance and recommendations
    - Vendor security assessment and third-party risk management procedures.
5. Third-Party Product and Vendor Listing
    - The vendor must provide a complete list of all third-party security products, partners, and tools used in their solution(s)
    - This list must include:
        - Remote Access and Administration Tools
        - Endpoint Detection and Response (EDR) solutions
        - Backup and Disaster Recovery (BDR) solutions
        - Cloud and email security tools including SOC monitoring
        - Privileged Access Management (PAM) Tools
        - Zero Trust and/or Privileged Access Management solutions
        - Any SASE Recommendations
        - Compliance and vulnerability assessment tools.

C. Pricing Proposal

- Fixed monthly pricing model for core services
- Licensing costs for MSP procured annual-based licensing
- Separate pricing for optional addons (24/7 help desk, compliance assessments, penetration testing, etc.)

D. References

- Three (3) references from aviation, transportation, or critical infrastructure clients.

T: 309.764.9621
F: 309.757.1515
2200 69th Ave. Suite 100
Moline, Illinois 61265
QCairport.com

Vendor Selection

The MAA will review all submitted proposals and determine which respondent(s) meets the needs of the airport's strategic objectives. As these needs may be served by multiple combinations, it will be the sole discretion of the Authority to determine which solution best serves the Quad Cities International Airport.

The Quad Cities International Airport recognizes that there may not be one perfect partner that meets all the needs. This RFP process is intended to help the MAA understand the capabilities and costs of the providers to determine if one or more providers are necessary in conjunction with internal resources to meet the objectives of the Information Technology function for the Quad Cities International Airport. Respondents are encouraged to provide the clearest understanding of their capabilities and limitations as possible, so that the MAA can determine if those capabilities fit into the overall strategy. Noted limitations in the RFP response, or absence of areas requested in the RFP, should not be considered a disqualification.

RFP Response Process

RFP Timeline

- March 17, 2025 – RFP Released to public
- March 28, 2025, 4:30PM CST – Deadline for questions regarding the RFP to be submitted to RFPs+IT@qcairport.com with the subject line "MSP RFP Question" (questions will not be accepted nor answered after this time).
- March 31, 2025 4:30PM CST – All submitted questions will be answered and posted on the website: https://www.qcairport.com/airport-business-home/airport-authority/public-notices-rfps/ NOTE: Aside from specialty areas such as licensing counts and software usage, we will not respond directly to questions from submitters. All answers will be posted on the website.
- April 17, 2025, 4:30PM – Deadline to submit an RFP response to RFPs+IT@qcairport.com with the subject line "MSP RFP Submission". Late submissions will not be accepted
- April 21 through May 23, 2025 – RFP response evaluations, follow-up questions with respondents, potential contract negotiations.
- July 1, 2025 – Target start date of new contract(s).

Questions regarding this RFP should be directed to RFPs+IT@qcairport.com and be submitted no later than March 28, 2025, 4:30PM CST. No individual at the airport should be contacted outside this email and timeline for information regarding this RFP, and any such action may negatively impact that vendor's standing in regard to the selection process. Answers to any questions will be posted on the website by May 11, 2025 at 4:30PM CST.

All RFP responses should be directed to RFPs+IT@qcairport.com with the subject line "MSP RFP Submission" prior to April 17, 2025, 4:30PM. Only written responses in the following computer document formats will be accepted: Microsoft Word (DOCX), Adobe PDF (PDF).

RFP respondents will be contacted after April 17 for any supplemental information, demonstrations, etc., if necessary. All respondents will be notified of standing by June 17.

T: 309.764.9621
F: 309.757.1515
2200 69th Ave. Suite 100
Moline, Illinois 61265
QCairport.com

Additional RFP Terms and Conditions

Please note the following additional terms and conditions of this RFP:

- The Metropolitan Airport Authority respects the confidentiality of every RFP response. Response information will not be shared with anyone outside of the RFP evaluation process and specifically not with other vendors without the express permission of the respondent.
- The Metropolitan Airport Authority reserves the right to adjust the schedule and RFP process at any time, provided public notice of this change is made.
- The Metropolitan Airport Authority may or may not enter contract negotiations with any respondent because of this RFP. It is the intent of the Metropolitan Airport Authority to satisfy its IT goals and needs and will do so at its discretion.

T: 309.764.9621
F: 309.757.1515
2200 69th Ave. Suite 100
Moline, Illinois 61265
QCairport.com