OHIO TURNPIKE AND
INFRASTRUCTURE COMMISSION

ADDENDUM NO. 2
ISSUED FEBRUARY 20, 2025

to

RFP NO. 5-2025
TO PROVIDE NETWORK OPERATIONS CENTER SERVICES

PROPOSAL DUE DATE: 5:00 P.M. (EASTERN TIME) MARCH 10, 2025

ATTENTION OF RESPONDENTS IS DIRECTED TO:

ANSWERS TO QUESTIONS RECEIVED THROUGH 5:00 PM ON FEBRUARY 17, 2025

-AND-

REVISED APPENDIX A – SCOPE OF SERVICES

Issued by the Ohio Turnpike and Infrastructure Commission through Aimee W. Lane, Esq, Director of Contracts Administration.

Aimee W. Lane

Aimee W. Lane, Esq.,
Director of Contracts Administration

February 20, 2025
Date

ANSWERS TO QUESTIONS RECEIVED THROUGH 5:00 P.M. ON FEBRUARY 17, 2025:

Q#11 Is there an incumbent partner for the Network Operation Center Services RFP?

A#11 No.

Q#12 Could you please provide the estimated budget for the Network Operation Center Services RFP?

A#12 A budget for NOC services has not been defined. The Commission is required by policy to award contracts under an RFP to the respondent with the proposal that offers the "best value" to the Commission in terms of service and price. As provided in the RFP, the Commission uses weighted scoring with the technical proposal counting for 70% of the combined score and the fee proposal counting for 30% of the combined score. The not-to-exceed amount for any resulting contract under this RFP will be based on the evaluation and scoring of the proposals received and contract negotiations with the top ranked firm. Additionally, the Commission does not provide budgetary information during a pending RFP due to statutory and policy requirements that require the Commission to procure the required services under a competitive proposal process.

Q#13 Will the Commission accept non-public sector references demonstrating experience with respect to the Scope of Services?

A#13 Yes.

Q#14 Please clarify how many years of audited financial statements should be provided.

A#14 The Commission wants the most recent two years of audited financial statement. If 2024 is not completed, the years 2022/2023 are acceptable.

Q#15 Would Ohio be open to the vendor handling the first-level resolution for incidents?

A#15 At this time, OTIC seeks a third party to assist only with monitoring and escalated incidents, per Appendix A section III. OTIC employs Technology staff for first-level resolution.

Q#16 What is the current ITSM system for NOC incidents?

A#16 NOC incidents may be tracked across multiple systems, but are not logged in a central ITSM system. OTIC is in the process of transitioning to a new ITSM system, ServiceDesk Plus.

Q#17 On average, what are the monthly incident counts for the network items? Please provide for the first level and second level (escalation).

A#17 OTIC seeks a third party to assist with escalated incidents only. Escalated incidents are expected to be fairly infrequent, at most a few times per month.

Q#18 What current discovery and monitoring tools are in place that we need to work with or replace?

A#18 OTIC is agnostic to the discovery and monitoring tools employed by the third party, provided the tools also meet the terms of the RFP. OTIC is not seeking a replacement for any current discovery or monitoring tools used by its internal IT staff.

Q#19 What CMDB or asset management tool is currently in use?

A#19 See Q#16; ServiceDesk Plus has CMBD capabilities that will be employed in the coming months.

Q#20 What are your current SLAs for the NOC?

A#20 OTIC is a 24/7/365 operation, so uptime is of critical importance for the core infrastructure. There are no documented SLAs currently.

Q#21 Do you have specific retention requirements for monitoring data beyond the 2-year minimum? Please describe.

A#21 Yes. The Commission is required to keep records related to network monitoring, specifically reports including incidents, equipment breakdowns, equipment repair, etc. for five (5) years. A revised copy of Appendix A – Scope of Services is included with this Addendum No. 2.

Q#22 What is your expected timeline for the NOC transition?

A#22 OTIC understands that the onboarding phase may vary depending on the third party's internal processes. Ideally, transition to support service would be completed within 3-6 months from the date of the awarded contract.

Q#23 The price for any cybersecurity service must account for an allocation of risk between parties. What limits can be established so that Service Providers are not subject to unlimited indemnification due to cybersecurity issues and events?

A#23 OTIC is not seeking cybersecurity service with this RFP. Regardless, as provided in PART VI, Item C of the RFP, Respondents should include any exceptions to the RFP, Scope of Services or form contract with the proposal. If the top ranked respondent included exceptions to the contract with its proposal, the Commission will attempt to negotiate those contract terms. If those contract negotiations are unsuccessful, the Commission with cease contract negotiations and commence contract negotiations with the next ranked respondent.

Q#24 Is the Commission willing to discuss indemnification obligations based on contract value or a fixed amount?

A#24 As provided in PART VI, Item C of the RFP, Respondents should include any exceptions to the RFP, Scope of Services or form contract with the proposal. If the top ranked respondent included exceptions to the contract with its proposal, the Commission will attempt to negotiate those contract terms. If those contract negotiations are unsuccessful, the Commission with cease contract negotiations and commence contract negotiations with the next ranked respondent.

Q#25 Is the Commission willing to discuss establishing a set number of years for survival instead of "forever"?

A#25 As provided in PART VI, Item C of the RFP, Respondents should include any exceptions to the RFP, Scope of Services or form contract with the proposal. If the top ranked respondent included exceptions to the contract with its proposal, the Commission will attempt to negotiate those contract terms. If those contract negotiations are unsuccessful, the Commission with cease contract negotiations and commence contract negotiations with the next ranked respondent.

Q#26 Our standard procedure is to monitor networks from multiple locations if multiple egress points exist. Does OTIC prefer to monitor the network from a single or multiple locations?

A#26 OTIC will work with the awarded vendor and agree upon the most appropriate method for monitoring, whether from single or multiple locations.

Q#27 Our preferred approach is to have available primary and secondary methods of connectivity for each monitoring location. Is OTIC comfortable with the resource utilizing LTE or Starlink solutions for out of band (OOB) connectivity?

A#27 Yes.

Q#28 Can you provide historical metrics on volume of incidents in the past year? And if possible, provide detail as to the volume of tickets which required remote engineering support and/or on-site break fix?

A#28 See Q#17.

Q#29 Are only the Incident/Event data (Tickets) required to be retained, or all performance data from monitoring tools?

A#29 Only Incident/Event data is required to be retained.

Q#30 What kind of service requests are currently being experienced? Is there any type of ticket log showing current request that the provider would be taking over? If so, can this be shared?

A#30 See Q#17. Due to the nature of this RFP and the need to maintain a secure environment, limited detail can be provided before a contract is awarded. OTIC will provide additional event, incident, configuration and documentation information to the awarded vendor during the discovery process.

Q#31 Are there any network drawings showing ISP information between sites?

A#31 See Q#30.

Q#32 Are there any vlan drawings that can be shared? Ideally looking for any drawings that explain how things are connected, down to the toll booths.

A#32 *See Q#30.*

Q#33 Can renewal dates/SmartNet dates for the cisco switches be shared?

A#33 See Q#9. Cisco support is maintained separately by OTIC and will be in place for all equipment in scope of this RFP.

Q#34 Does the Turnpike Commission have equipment (servers/virtual servers) that could be used to deploy windows based monitoring agent?

A#34 Yes.

Q#35 How many people currently work in IT for the Turnpike Commission that might be escalating issues?

A#35 10-15 OTIC technology employees may be involved in ticket escalations at varying levels, from Technician to department director.

Q#36 How does the Turnpike Commission measure contract performance?

A#36 Performance is measured by whether the select firm performs the services set forth in Appendix A, Scope of Services, and complies with the submitted proposal and terms of any signed contracts.

Q#37 Would the Turnpike Commission be upgrading equipment soon?

A#37 No; in February 2024, a project to replace all OTIC fiber and ethernet network equipment was completed.

Q#38 What are the security requirements for the network?

A#38 See Appendix A for information about security requirements pertaining to this RFP.

Q#39 Are there any compliance standards that need to be adhered to?

A#39 OTIC maintains compliance with NIST-CSF and PCI-DSS 4.0.

Q#40 Are there any pending projects/upgrades scheduled to be completed?

A#40 See Q#37.

Q#41 Do all locations tie back to the Admin complex via MPLS, bovpn, etc.?

A#41 See Q#30.

Q#42 What is the primary role of your NCS routers within your network? Are they being used in a core, edge, or aggregation role?

A#42 See Q#30.

Q#43 What specific requirements led to the selection of these routers—high throughput, MPLS, segment routing, optical transport, or other factors?

A#43 See Q#30.

Q#44 Are they supporting a service provider environment, data center interconnect, or another specialized use case?

A#44 See Q#30.

Q#45 What features of the NCS platform are most critical to your operations (high-density interfaces, segment routing, automation, optical integration, etc.)?

A#45 See Q#4, Q#20 and Q#30.

Q#46 Do they require management of IOS XR and advanced routing technologies such as MPLS, BGP, EVPN, or SR-MPLS?

A#46 See Q#30.

Q#47 Are the routers integrated with an SDN or automation framework, and if so, what tools are currently in use (Cisco Crosswork, Ansible, NetConf/RESTConf APIs, etc.)?

A#47 See Q#30.

Q#48 What are your key operational priorities for these routers (e.g., performance optimization, security hardening, lifecycle management)?

A#48 See Q#30.

Q#49 Are there any plans for future expansion or modifications to your NCS deployment?

A#49 See Q#4.

Q#50 How are the in-scope network devices being managed and patched (firmware updates) today? Are you using a centralized management console?

A#50 See Q#30.

Q#51 Regarding the Annual 24x7x365 Support Services (Appendix A, Section II), is a continuously staffed help desk required, or can network alerts be managed by on-call engineers?

A#51 Automation can be leveraged in place of a continuously staffed service desk. Refer to Q#20; resource availability is critical to our operation in the event of an escalation.

Q#52 Does OTIC have staff available on-site after regular business hours to assist with network troubleshooting?

A#52 See Q#15. OTIC staff will be available for diagnosis and troubleshooting of network equipment based on urgency. Should incidents occur after regular business hours, OTIC staff will be available as needed.

Q#53 Does OTIC typically procure its own network hardware and maintenance, or is this managed through a separate arrangement?

A#53 OTIC procures its own network hardware and maintenance.

Q#54 Would you be able to host a walkthrough of your network environment?

A#54 A walkthrough of the network environment will take place during the onboarding phase of the engagement.

Q#55 What level of support is needed from provider or the "extra" services referenced in Appendix A Scope of Services? Do you want to look at the cybersecurity retainer option?

A#55 Per Appendix A Section IV, additional services will be scoped and quoted on a task order basis.

Q#56 What is the expected timeline for the takeover process?

A#56 See Q#22.

Q#57 How many engineers are currently available to support this engagement?

A#57 See Q#35.

Q#58 What is the estimated level of effort per device (e.g., per week)?

A#58 See Q#17 and Q#30.

Q#59 Are there any known constraints in expertise (e.g., specific vendors, models, or software versions)?

A#59 OTIC seeks a third party to assist with escalated incidents, not to supplement current Technology staff expertise.

Q#60 Will this be a 24/7 support engagement, or is it business hours only?

A#60 See Appendix A; this is expected to be a mix of business hours and 24/7 support as needed. See Q#20.

Q#61 Are there any Service Level Agreements (SLAs) that must be met?

A#61 See Q#20.

Q#62 Will additional training or certifications be required for the team?

A#62 See evaluation scoring table; respondents should provide "skills, reputation, experience, capabilities and expertise in performing the required services" and "Qualifications of the individuals proposed to perform services."

Q#63 Is there an escalation process in place for critical issues?

A#63 OTIC will work with the awarded vendor and agree upon an escalation process for critical issues.

Q#64 Who will be responsible for knowledge transfer and documentation handoff?

A#64 See Q#5.

Q#65 What is the current firmware/software patching strategy, and when was the last update applied?

A#65 See Q#30.

Q#66 Are there any known hardware or software end-of-life (EOL) or end-of-support (EOS) concerns?

A#66 See Q#33 and Q#37.

Q#67 What is the current high availability (HA) configuration of these firewalls?

A#67 See Q#30.

Q#68 Are there any firewall rules or configurations flagged as non-compliant or out-of-policy?

A#68 See Q#30.

Q#69 What logging and monitoring tools are integrated with these firewalls?

A#69 See Q#30.

Q#70 Are there any outstanding vulnerabilities that need immediate patching?

A#70 See Q#30.

Q#71 Are there any firewall rule cleanup or optimization tasks that need attention?

A#71 See Q#30.

Q#72 How many firewall-related support tickets have been opened in the past 30, 60, and 90 days?

A#72 See Q#17.

Q#73 What are the primary categories of these tickets? (e.g., performance, connectivity, misconfiguration, security events)

A#73 See Q#30.

Q#74 How many of these tickets remain unresolved or are frequently re-opened?

A#74 See Q#30.

Q#75 Are there any recurring patterns or high-priority issues that require attention?

A#75 See Q#30.

Q#76 What are the most severe incidents that have occurred in the past 6 months?

A#76 See Q#30.

Q#77 How are tickets currently prioritized and assigned?

A#77 See Q#17.

Q#78 Is there an existing knowledge base for handling common issues?

A#78 See Q#5.

Q#79 What is the average resolution time for firewall-related tickets?

A#79 See Q#17 and Q#30.

Q#80 What is the current change management process for firewall updates and modifications?

A#80 See Q#30.

Q#81 How frequently are firewall policy or rule changes requested?

A#81 See Q#30.

Q#82 What are the approval workflows for making firewall changes?

A#82 See Q#30.

Q#83 Are there any pending firewall-related change requests in the pipeline?

A#83 See Q#30.

Q#84 What is the rollback strategy for failed firewall changes?

A#84 See Q#30.

Q#85 Are firewall changes documented in a central repository?

A#85 See Q#16 and Q#19.

Q#86 Are there any regulatory compliance requirements that impact firewall management? (e.g., PCI-DSS, NIST, ISO 27001)

A#86 See Q#39.

Q#87 What network and security infrastructure components are dependent on these firewalls? (e.g., SD-WAN, VPNs, IPS/IDS, cloud security)

A#87 See Q#30.

Q#88 Are there any third-party integrations that need to be considered?

A#88 See Q#30.

Q#89 What authentication methods are used for firewall administration? (e.g., local accounts, RADIUS, TACACS+

A#89 See Q#30.

Q#90 Are firewall backups and configurations regularly stored and version-controlled?

A#90 See Q#30.

Q#91 Are there any interdependencies with other managed security services?

A#91 No.

Q#92 Are there any known gaps in documentation that will hinder a smooth takeover?

A#92 See Q#5.

Q#93 Will this require support from a FISMA High support model?

A#93 FISMA does not apply to this RFP.

Q#94 Is this a staff augment for the Commission NOC or do they want “dedicated” OC resources. If yes, is this 24X7 or a specified time & day of week?

A#94 This RFP is not for OTIC Technology staff augmentation.

Q#95 Will this require any type of troubleshooting and remediation of identified events/alerts? Appendix A section II

A#95 Troubleshooting and remediation assistance may be required for identified events per Appendix A, Section III. See also Q#15.

Q#96 Is the network monitoring Device Up/Down only?

A#96 See Q#18.

Q#97 If real-time network event notifications upon occurrence based on an agreed upon impact and urgency matrix - is matrix already defined? If so, please share.

A#97 No. The matrix will be agreed upon with the awarded vendor.

Q#98 Is there an expectation of monitoring transport circuits connected to the network HW? If yes, what type of transport circuits do they have & with which carrier?

A#98 This RFP is for NOC services related to the hardware described in Appendix A. Transport monitoring can be limited to up/down for applicable hardware; no additional monitoring of internet circuits will be required.

Q#99 What are detailed expectations of skills/functions for the Remote Engineer request? Are there expectations of skills on HW outside of the list in the RFP? Appendix A section III

A#99 The awarded vendor should be able to provide support for escalated incidents applicable to the hardware defined in the RFP's scope.

Q#100 Please provide clarity on what level of security audit the provider's tools must pass? Appendix A bottom of section III states "The monitoring, service desk and inventory tracking systems in use by the resource must be demonstrated as having robust security to best protect the Turnpike's infrastructure. The resource must have a security and continuity of business plan in place and provide documentation to the Turnpike as needed and when updated."

A#100 OTIC seeks respondents to attest to maintaining robust security measures. Evidence of this can be provided in the respondents proposal, which will be rated according to the RFP scoring guidelines.

END OF ADDENDUM NO. 2

REVISED APPENDIX A- SCOPE OF SERVICES

The Ohio Turnpike is seeking a dedicated resource to provide Network Operations Center ("NOC") monitoring and remote engineering support for the Turnpike's Fiber (DWDM) and Ethernet networks.

I. To familiarize the resource with the environment, it is required that an initial onboarding/discovery phase be executed to fully understand the network. This would include but is not limited to:

- Use of network discovery tools to identify network components
- Review of existing infrastructure documentation provided by Turnpike staff
- Interviews/discussions with key Turnpike staff

II. Following onboarding, the resource would be responsible for providing the following services on a 24/7/365 basis:

- **Network / equipment monitoring:** The resource will monitor all Turnpike equipment in scope to the agreement. Network monitoring software may be provided by the resource and installed on Turnpike equipment to facilitate this monitoring.

- **Network event notifications (event and incident management):** The resource will provide real-time network event notifications upon occurrence based on an agreed upon impact and urgency matrix; these notifications may be automated by network monitoring software. Events/incidents that are reported will be logged in and managed by the resource's service desk system; designated Turnpike staff will be provided access to the service desk system to check status of past or current incidents. Trend analysis will be conducted on an as-needed basis for common/recurring incidents that require a more thorough root-cause analysis. Retention of incident/event documentation by the resource is required for a period of at least 5 ~~2~~ years.

III. Following onboarding, the resource would be responsible for providing the following services on an as-needed basis, which could include after-hours support:

- **Remote engineering and service desk for escalated network incidents:** The resource will be available to provide support for escalated incidents and will provide an escalation matrix for Turnpike staff use. Turnpike staff will provide initial support for reported incidents, including on-site diagnostic if required. In the event Turnpike staff is unable to resolve an incident, or requires additional support, the resource would provide subject matter expertise to aid in the resolution of incidents.

Following onboarding, the resource would be responsible for providing the following services on an 8 x 5 basis, Monday through Friday:

- **Support for inventory control / change management requirements:** The resource will help monitor the overall health of network equipment by monitoring equipment age, firmware versions, and recommend to Turnpike staff when upgrades should be completed. During such upgrades, the resource will be available to support Turnpike staff if required.

- **Periodic reviews / health checks / status updates:** The resource will be available for periodic (up to quarterly) customer reviews to discuss issues, trends, upcoming projects and other items that may impact service delivery. The resource will make available periodic status reports for Turnpike management to monitor the overall performance and efficacy of the program.

IV. Additional services not listed above will be quoted by the resource on a task-order basis upon request, including but not limited to onsite break/fix support, network design consulting, project/implementation support, security incident support, and other consulting services to address the strategic needs of the Turnpike's technology footprint. The resource will include hourly rates for these services in their proposal.

All services would be provided according to agreed upon SLAs based upon impact and urgency.

The monitoring, service desk and inventory tracking systems in use by the resource must be demonstrated as having robust security to best protect the Turnpike's infrastructure. The resource must have a security and continuity of business plan in place and provide documentation to the Turnpike as needed and when updated. Additionally, the resource will follow Turnpike security policies as defined in the Information Security Policy (which will be provided only after a contract is awarded).

The following is a current summary of the equipment in place across the Turnpike Fiber and Ethernet networks:

2 – Cisco Firepower 2130 with FTD
2 – Cisco Firepower 4145 with FTD
2 – Cisco Nexus 93180
2 – Cisco Catalyst 9410
2 – Cisco Catalyst 9600
26 – Cisco NCS 560-4 RSP4 Router
14 – Cisco NCS 5504
2 – Cisco NCS 540X-12Z16G-SYS-D Router
37 – Cisco Meraki CW9164I
55 – Cisco Catalyst 9300-48UXM
58 – Cisco Catalyst 9330-24P
37 – Cradlepoint R2105

As the OTIC network changes, service fees may be adjusted accordingly. In the proposal, the resource will provide an itemized (management fees, license fees, etc) structure for cost changes based upon the addition or removal of equipment over the length of the contract.