MATANUSKA-SUSITNA BOROUGH ACTION MEMORANDUM **AM No. 26-031**

SUBJECT: Award of proposal number 26-081P to Koniag Cyber Solutions, LLC for the three-year contract amount of $526,833.00 to provide Cyber Security Managed Detection and Response Services.

AGENDA OF: March 17, 2026

ASSEMBLY ACTION:

AGENDA ACTION REQUESTED: Present to the Assembly for consideration.

Route To:	Signature
Purchasing Director	X Rustin Krafft Signed by: Russ Krafft 3/4/2026
Information Technology Director	Recoverable Signature X Leah Jones Signed by: Leah Jones
Finance Director	Recoverable Signature X Cheyenne Heindel Signed by: Cheyenne Heindel
Borough Attorney	X Nicholas Spiropoulos Signed by: Nicholas Spiropoulos 3/4/2026
Borough Manager	X Michael Brown Signed by: Mike Brown 3/4/2026
Borough Clerk	Recoverable Signature X Lonnie McKechnie Signed by: Lonnie McKechnie

ATTACHMENT(S): Analysis Sheet (1p)
Scope of Services (4p)

SUMMARY STATEMENT: On November 6, 2025, the Matanuska-Susitna Borough Purchasing Division issued a solicitation requesting proposals from qualified firms to provide Cyber Security Managed Detection and Response Services. This contract will allow the Borough Information Technology staff to proactively reduce cybersecurity risks, protect sensitive and critical information, and prevent disruptions to essential public services. These services strengthen the Borough's ability to detect and respond to cyber incidents in a timely manner, reduce potential financial and operational impacts, and support the Assembly's responsibility to safeguard public assets and maintain public trust in Borough operations.

Services purchased will support the Information Technology

Department for all assembly districts.

In response to the advertisement, seventeen proposals were received. A proposal evaluation team made up of Borough Information Technology Staff evaluated the proposals and selected Koniag Cyber Solutions, LLC as the most advantageous firm for the Borough.

The initial contract period of performance begins upon execution of the contract and ends on June 30, 2027. The term of this agreement is one year, with two additional one-year renewals (potentially a three-year contract), subject to annual appropriation of funds by the Borough Assembly.

In accordance with MSB 3.08.170(B), Administration requests authority to modify the resulting contract completion date by 90 days for unforeseen circumstances.

The Information Technology Department, Infrastructure/Security Division will be administering the contract.

RECOMMENDATION OF ADMINISTRATION: Approve the subject action memorandum.

MATANUSKA-SUSITNA BOROUGH
FISCAL NOTE
Agenda Date: March 17, 2026

SUBJECT: Award of proposal number 26-081P to Koniag Cyber Solutions, LLC for the three-year contract amount of $526,833.00 to provide Cyber Security Managed Detection and Response Services.

FISCAL ACTION (TO BE COMPLETED BY FINANCE)	FISCAL IMPACT **YES** NO
AMOUNT REQUESTED $526,833*	FUNDING SOURCE FY27 IT Operating Budget
FROM ACCOUNT # 100.115.122 4xx.xxx	PROJECT
TO ACCOUNT :	PROJECT #
VERIFIED BY: 3/4/2026 X Liesel Zanto Signed by: Liesel Zanto	CERTIFIED BY:
DATE:	DATE:

EXPENDITURES/REVENUES: (Thousands of Dollars)

OPERATING	FY2026	FY2027	FY2028	FY2029	FY2030	FY2031
Personnel Services						
Travel						
Contractual		526.8* →				
Supplies						
Equipment						
Land/Structures						
Grants, Claims						
Miscellaneous						
TOTAL OPERATING		526.8* →				
CAPITAL						
REVENUE						

FUNDING: (Thousands of Dollars)

General Fund		526.8* →				
State/Federal Funds						
Other						
TOTAL		526.8* →				

POSITIONS:

Full-Time						
Part-Time						
Temporary						

ANALYSIS: (Attach a separate page if necessary) *Subject to approval of Annual budgets

PREPARED BY: _____ PHONE: _____

DEPARTMENT: _____ DATE: _____

Recoverable Signature

X Cheyenne Heindel

APPROVED BY: Signed by: Cheyenne Heindel DATE: _____

AM No. 26-031

26-081P Cyber Security Managed Detection and Response Service

Scoring Summary

	C - Evaluation Phase 3: Presentations	C-1 - Software Fit and Functional Capability	C-2 - Implementation Readiness and Support	C-3 - Presentation Quality and Team Expertise
Supplier	**/ 100 pts**	**/ 50 pts**	**/ 30 pts**	**/ 20 pts**
Koniag Cyber Solutions	81.2 pts	44 pts	22.8 pts	14.4 pts
Scopewell Solutions	75.6 pts	42 pts	16.8 pts	16.8 pts
World Wide Technology	63.2 pts	32 pts	16.8 pts	14.4 pts
Computer Task Group, Inc.	52.8 pts	24 pts	16.8 pts	12 pts
Golden Five LLC	52.8 pts	24 pts	16.8 pts	12 pts

SCOPE OF SERVICES

26-081P, CYBER SECURITY MANAGED DETECTION AND RESPONSE SERVICE

1 Statement of Work

1.1 Purpose

The purpose of this Request for Proposal (RFP) is to invite prospective vendors to submit a proposal to supply a Managed Detection and Response Service (MDR) to Matanuska-Susitna Borough (MSB). The RFP provides vendors with the relevant organizational, operational, service and performance, system, and architectural requirements of an MDR.

1.2 Coverage and Participation

The intended coverage of this RFP, and any agreement resulting from this solicitation, shall be for the use of all departments at MSB and any of its satellite offices. MSB reserves the right to add and/or delete elements or to change any element of the coverage and participation at any time without prior notification and without any liability or obligation of any kind or amount.

1.3 Period of Performance

The intended period of performance will be June 1, 2026, through June 30, 2029. The award of this contract will be contingent upon approval of the FY27 budget. A break-out of the cost per year will be required with an option to renew yearly after original contract. Contract will include a proof of concept of 30-90 days before June 1, 2026.

1.4 The MSB anticipates annual services for this contract to cost less than $175,000.

2 General Information

2.1 Original RFP Document

MSB shall retain the RFP and all related terms and conditions, exhibits, and other attachments, in original form in an archival copy.

2.2 The Enterprise

The Matanuska-Susitna Borough (MSB) is committed to strengthening its security posture to address today's intricate and evolving cyber threat landscape. The requirements outlined in this document combine the Borough's business and technical objectives, project scope, and desired features, including both functional specifications and workflow expectations, to ensure protection of MSB's digital assets, sensitive data, and critical infrastructure.

The goals of the Managed Detection and Response Service include enhancing threat and vulnerability management capabilities, improving security device management with integrated monitoring, ensuring comprehensive auditing and compliance, and streamlining incident response processes. Additionally, the service should facilitate ongoing staff training and skill development. MSB wants to minimize the organization's exposure to security risk and enhance its overall security posture. In addition, we want to improve the accuracy and reliability of security processes that also minimize errors and inconsistencies.

2.3 Proposal Variations:

Vendors are encouraged to submit multiple proposals if desired, to reflect different service tiers, scalability options, or pricing models. This flexibility will allow the Borough to evaluate solutions that best align with current and future needs. Vendors will be limited to two proposals.

2.4 Existing Technology Environment

The following is a listing of our current technology environment.

Microsoft Defender, Microsoft Purview, Firewall, Routers and Switches, Windows Servers and Desktops, Linux Servers and Desktops, Mac Devices, iOS Devices, Virtualization, Solar Winds (optional).

If the proposed solution includes or integrates with Microsoft Sentinel, vendors should note that the Matanuska-Susitna Borough will procure Sentinel licensing separately. Vendors should not include Sentinel licensing costs in their pricing proposals; however, the cost of that software will be factored into the vendor's total contract amount when evaluating proposals.

3 Scope of Work, Specifications, and Requirements

The service must be scalable across all MSB locations and infrastructure, supporting on-premise, cloud, co-managed, or hybrid architectures, with vendor recommendations on the best approach. It should provide monitoring of Outlook email environments with rapid detection and response to phishing, malware, and other suspicious activities, as well as integrate smoothly with existing MSB infrastructure while allowing for future growth. The service should include optional periodic penetration testing with reporting and remediation recommendations, comprehensive incident management covering containment, remediation, and root cause analysis, and robust training for Borough IT staff via the MSB's training platform.

3.1 Service Management

1. **SLA Management**
   - Describe the process by which formal SLA for managed security services is being established.
   - Describe the process by which SLA is being monitored and evaluated.
   - Describe the process by which SLA is being reviewed and improved.
2. **Service Report**
   - Indicate the types of service reports that are provided.
   - Describe the process by which service reports are being generated and submitted.
   - Indicate the types of communication channels that are provided, such as onsite meeting and conference meeting.

3.2 Service Features

1. **Capability of Real-Time Monitoring and Analysis**
   - Indicate whether your service supports real-time security event and log monitoring and analysis.
   - If the answer is "yes," describe the process/factor by which the capability is provided.
2. **Onsite Incident Response Support**
   - Indicate whether your service supports onsite incident response.
   - If the answer is "yes," describe the process/factor by which the capability is provided.
3. **Services Support Multiple Vendors' Products**
   - Indicate whether your service supports multiple vendors' products.
   - If the answer is "yes," describe the process/factor by which the capability is provided.
4. **In-Depth Technical and Security Request Support**
   - Indicate whether your service supports in-depth technical and security requests.
   - If the answer is "yes," describe the process/factor by which the capability is provided.
5. **Real-Time View Through Flexible Client Interface**
   - Indicate whether your service supports real-time view through flexible client interface.
   - If the answer is "yes," describe the process/factor by which the capability is provided.

6. Dedicated Team per Client

- Indicate whether your service supports dedicated team per client.
- If the answer is "yes," describe the process/factor by which the capability is provided.

7. Support Compliance Audit and Assessment

- Indicate whether your service supports compliance audit and assessment.
- If the answer is "yes," describe the process/factor by which the capability is provided.

8. 24x7x365, Multiple, Redundant SOCs With Disaster Recovery and Global Coverage

- Indicate whether your organization has multiple, redundant SOCs with disaster recovery and global coverage.
- If the answer is "yes," describe the process/factor by which the capability is provided.

9. Global Online Community Providing Insight and Intelligence

- Indicate whether your organization has a global online community providing insight and intelligence.
- If the answer is "yes," describe the process/factor by which the capability is provided.

3.3 Service Operations

1. Implementation and Configuration

Proposals should provide a detailed service scope that clarifies all included features and capabilities, along with clear implementation timelines covering each phase from initial assessment to full operational deployment. They must outline transition plans for ongoing management by existing staff in cases where a dedicated IT security team is unavailable, and state any assumptions regarding feature gaps or limitations. The submission should also specify arrangements for ongoing support and maintenance. Furthermore, proposals need to describe how the product integrates with Microsoft Defender endpoint, or if the service uses its own endpoint protection, how it avoids conflicts with the built-in Microsoft tools. Additionally, there should be a comprehensive explanation of how the product works with Windows Defender Online logging from both workstations and servers.

- Describe the process by which functional security devices for your services are deployed. Include any tasks that must be performed on systems or devices already deployed (e.g. network configuration and third-party integration).
- Describe the process by which the security management device/appliance for your service is deployed. Include any tasks that must be performed on systems or devices already deployed.
- Describe the process by which the security reporting device/appliance for your service is deployed. Include any tasks that must be performed on systems or devices already deployed.

2. Ongoing Operations

- Describe the process by which the initial configuration of your service is performed. Include the implementation of any necessary security devices, the creation of any rules, and the configuration of any and all settings required for optimal operations.
- Describe the process by which the initial configuration of your service is updated and maintained. Include the update of any necessary security devices, the update and/or modification of any rules, etc.

3. Auditing and Reporting

- Describe the logging capabilities for security devices. Address both onsite logging capabilities (within our organization's perimeter) and offsite logging capabilities (within MDR's perimeter). Indicate the type of data that can be captured as well as all protection and control mechanisms that are applied to the logs (including log encryption, log access restrictions, etc.).

- Describe the auditing and reporting capabilities for captured logs. Address whether standard report templates exist, whether they must be constructed, or whether the system supports ad hoc reporting only. Where standard templates exist, indicate what types of reports they represent and in all cases indicate what types of information can be presented in reports.

3.4 Service Support

Describe how you work with clients to deliver services.

1. **Customer Support**
   - Do you provide toll-free customer support 24 hours a day, seven days a week? Please specify all paid support options.

2. **Implementation Support**
   - Do you provide complete turnkey, onsite implementation and project management support? Please specify which support will be included and which is provided for an additional fee. Also specify whether support is available directly from the vendor or provided through a partner.

3.5 Questionnaire attachments

Fill out the attached questionnaires & submit with the proposal.

END OF SCOPE