City of Raleigh

Request for Proposals #: 274-*RPD3-25*

Title: Intelligence Management/Development Software

Proposal Due Date and Time: March 24, 2025
no later than 5:00 PM EST

ADDENDUM NO. *# 1*

Issue Date: February 21, 2025

Issuing Department: Raleigh Police Department
Direct all inquiries concerning this RFP to:

Captain Charles Penny
Title: Captain Raleigh Police Department
Email: Charles.Penny@raleighnc.gov

Addendum # *1* to RFP 274-RPD3-25 Intelligence Management/Development Software

Issue Date: February 21, 2025

To: All Proposers

This Addendum, containing the following Vendor Security Questionnaire v2, is issued prior to receipt of proposal packages and does hereby become part of the original RFP documents and supersedes the original RFP documents in case of conflict.

Receipt of this addendum must be acknowledged by signing in the area indicated below. Please complete the attached Vendor Security Questionnaire v2 to the RFP as listed below and **sign and return this addendum with your proposal package**.

Please complete the vendor identification section and then respond to all questions on the attached City of Raleigh Vendor Security Questionnaire v2

Captain Charles Penny
Raleigh Police Department

Sign below and return this addendum with your proposal.

Proposer Name & Company: _____ Date: _____

Signature: _____ Title: _____

City of Raleigh Vendor Security Questionnaire v2

Vendor to complete vendor identification section and then respond to all questions. Some rows may be hidden; you do not need to respond to hidden questions. If documents are requested please use "Insert object" to attach the document directly into the Vendor Comments cell.

Company Name:	
Company Address:	
Security officer contact information:	
Completed By:	
Date Completed:	

#	Question	Risk Baseline	Vendor Response - please select from dropdown	Vendor Comments
1	**Document Requests**			
1.1	Does your organization have a SOC 2 Type I or Type II report, a SOC 3 Type II report, or ISO 27001 certification that is less than 12 months old? If Yes and it is a SOC 2 Type I, please provide a copy of the report, skip to Section 4, and complete the remainder of the questionnaire If Yes and it is a SOC 2 Type II, please provide a copy of the report, skip to Section 11, and complete the remainder of the questionnaire If Yes and it is a SOC 3 Type II report, please provide a copy of the report, skip to Section 9, and complete the remainder of the questionnaire. If Yes and it is an ISO 27001 certification, please provide a copy of the certificate, skip to Section 11, and complete the remainder of the questionnaire. If No, please complete the full questionnaire	N/A		
1.2	Please provide a copy of your information security policy	N/A		
1.3	Please provide a copy of any information security or privacy certifications (e.g. ISO 27001, PCI DSS, GDPR)	N/A		
1.4	Please provide a copy of any relevant audit reports that cover information security controls (e.g. NIST CSF audit)	N/A		
1.5	Please provide a copy of your latest penetration test and/or vulnerability assessment report	N/A		
2	**Asset Management - Identifies, tracks, and safeguards hardware, software, and data assets throughout their lifecycle**			
2.1	Do you maintain an inventory of all hardware and software assets, including ownership?	HIGH		
2.2	Do you have an information classification scheme and process designed to ensure that information is protected according to its confidentiality requirements?	HIGH		
2.3	Do you maintain an inventory or map of data flows between both internal and external information systems?	HIGH		

3	**Governance - Establishes policies, procedures, and oversight to ensure alignment between security practices and organizational goals**			
3.1	Do you have an information security policy that has been approved by management and communicated to all applicable parties?	HIGH		
3.2	Do you have an information security policy exception process that includes formal acceptance of risk by the risk owner?	HIGH		
3.3	Do you have a process for reviewing your information security policy at least annually?	MEDIUM		
3.4	Do you regularly perform security threat and risk assessments on critical information systems using an industry-standard risk assessment methodology?	HIGH		
3.5	Have you designated an individual, who is at least at a manager level, who is responsible for information security activities?	HIGH		
3.6	Do you have a process designed to monitor changes to regulations and ensure compliance with relevant security requirements?	MEDIUM		
4	**Supply Chain Risk Management - Evaluates and mitigates risks associated with third-party vendors, suppliers, and partners**			
4.1	Do you perform security assessments on potential suppliers prior to entering into agreements with them?	MEDIUM		
4.2	Do your agreements with suppliers include appropriate measures designed to meet security requirements and assign shared responsibility?	MEDIUM		
4.3	Do you regularly evaluate suppliers to ensure that they are meeting their security obligations?	MEDIUM		
5	**Identity Management, Authentication, and Access Control - Manages user identities and ensures only authorized individuals have access to systems and data, including systems created and maintained by the company, as well as third party systems used by the company in the day-to-day operations of the business**			
5.1	Is all access to information systems formally approved by the appropriate asset owner?	MEDIUM		
5.2	Can all access to information systems be traced to unique individuals?	HIGH		
5.3	Are all access rights to information systems regularly reviewed for appropriateness by the asset owners?	MEDIUM		
5.4	Are all access rights to information systems immediately revoked upon employee/contractor termination or change of role?	HIGH		
5.5	Do you restrict and control the use of privileged accounts through the use of a Privileged Account Management system or equivalent controls?	HIGH		
5.6	Do you manage access permissions and authorizations, incorporating the principles of least privilege and separation of duties?	HIGH		
5.7	Do you require the use of multi-factor authentication for all remote access to organizational data, including email?	HIGH		
5.8	Do you require the use of multi-factor authentication for all administrative access to cloud-based information systems?	MEDIUM		
6	**Human Resource Security - Ensures employees, contractors, and third parties are aware of and adhere to security responsibilities before, during, and after employment**			
6.1	Do you have an information security awareness program designed to ensure that all employees and contractors receive security education at least yearly as relevant to their job function?	HIGH		

6.2	Do you conduct regular phishing simulation tests of your employees?	HIGH		
6.3	Do you conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for?	HIGH		
6.4	Do you require all new employees and contractors to sign confidentiality agreements?	MEDIUM		
7	**Data Security - Protects sensitive data from unauthorized access, loss, or alteration through encryption, classification, and controls, including systems created and maintained by the company, as well as third party systems used by the company in the day-to-day operations of the business**			
7.1	Do you require that all removable media, which may contain organizational data, is encrypted?	MEDIUM		
7.2	Do you require that all media, including hardcopies, containing organizational data is disposed of securely when no longer required?	HIGH		
7.3	Have you implemented data loss prevention (DLP) tools?	HIGH		
7.4	Do you employ full disk encryption on all laptops?	MEDIUM		
7.5	Do you encrypt databases?	HIGH		
8	**System Acquisition, Development, and Maintenance - Incorporates security requirements into the procurement, development, and maintenance of IT systems**			
8.1	Are information security requirements defined for all new information systems, whether acquired or developed?	MEDIUM		
8.2	Are development and testing environments separate from the production environment?	HIGH		
8.3	Is data used for development and testing protected through anonymization?	HIGH		
8.4	Are information security requirements tested to ensure that they function as designed?	HGH		
8.5	Are your applications developed with secure coding practices, including the OWASP Top 10 Most Critical Web Application Security Risks?	HIGH		
8.6	Are your web applications protected by an application layer firewall?	HIGH		
8.7	Do you incorporate threat modeling into application design?	MEDIUM		
8.8	Is application source code tested for vulnerabilities using source code reviews or static application security testing?	HIGH		
8.9	Are new information systems scanned for vulnerabilities prior to deployment?	HIGH		
8.10	Do you monitor and restrict the installation of unauthorized software?	HIGH		
9	**Physical and Environmental Security - Safeguards physical infrastructure and facilities against unauthorized access and environmental threats**			
9.1	Are physical security perimeter controls implemented around sensitive locations such as data centers?	HIGH		
9.2	Are all visitors appropriately identified, logged, and escorted while in sensitive locations?	HIGH		
10	**Information Protection Processes and Procedures - Establishes formal processes for the consistent protection of information and compliance with security policies**			
10.1	Are security configuration baselines defined and implemented for all endpoints and network devices?	MEDIUM		
10.2	Do you use automated tools to verify that endpoints and network devices comply with their baselines?	MEDIUM		

10.3	Do you segregate your network into zones based on trust levels, and control the flow of traffic between zones?	MEDIUM		
10.4	Do you control the transfer of information to external parties through authentication and encryption?	HIGH		
10.5	Are all changes to information systems recorded, planned, and tested (e.g., via a Change Approval Board (CAB) process)?	HIGH		
10.6	Are all information systems that are susceptible to malware protected by up-to-date anti-malware software?	HIGH		
10.7	Do you have a backup and recovery process designed to ensure that data can be recovered in the event of unexpected loss?	HIGH		
10.8	Do you segregate wireless network access for BYOD and guest access from your production network?	MEDIUM		
10.9	Do you enforce containerization on all mobile devices that may contain organizational data, including email, whether those devices are owned by the organization or by employees?	MEDIUM		
10.10	Do you have the capability of deleting all organizational data from laptops and mobile devices, whether owned by the organization or by employees, in the event that the device is lost or stolen?	HIGH		
10.11	Do you monitor external sources, such as vendor bulletins, for newly identified vulnerabilities and patches?	MEDIUM		
10.12	Do you evaluate, test, and apply information system patches in a timely fashion according to their risk?	HIGH		
11	**Protective Technology - Utilizes tools and technologies to defend systems and data from cyber threats, including systems created and maintained by the company, as well as third party systems used by the company in the day-to-day operations of the business**			
11.1	Have security event logging requirements been defined, and are all information systems configured to meet logging requirements?	MEDIUM		
11.2	Are security event logs protected and retained per defined logging requirements?	MEDIUM		
11.3	Have you deployed intrusion detection or prevention systems at the network perimeter?	MEDIUM		
11.4	Have you deployed tools to limit web browsing activity based on URL categories?	MEDIUM		
11.5	Have you deployed controls to detect and mitigate denial of service attacks?	HIGH		
12	**Security Continuous Monitoring - Continuously monitors systems and networks to identify vulnerabilities and detect potential security incidents**			
12.1	Have you deployed automated tools to collect, correlate, and analyze security event logs from multiple sources for anomalies?	MEDIUM		
12.2	Do you monitor privileged user activity to detect potential security events?	MEDIUM		
12.3	Do you monitor user activity to detect potential security events?	HIGH		
12.4	Are security alerts monitored 24x7?	HIGH		
12.5	Do you employ automated tools to scan information systems for vulnerabilities on a regular basis?	HIGH		
12.6	Do you perform penetration tests on all web applications and services, in accordance with standard penetration testing methodologies on at least an annual basis?	HIGH		
13	**Information Security Incident Management - Prepares for, detects, and responds to security incidents to minimize impact and facilitate recovery**			
13.1	Do you have a formal, documented security incident response plan?	HIGH		

13.2	Do you conduct regular tests of your security incident response plan?	HIGH		
13.3	Are all security incidents recorded, classified, and tracked?	HIGH		
13.4	Are forensic investigations conducted as part of incident response?	HIGH		
14	**Privacy - Ensures the ethical and legal handling of personal and sensitive information to protect individual rights**			
14.1	Do you have a data retention policy and process that is designed to meet relevant privacy regulations?	HIGH		
14.2	Do you maintain an inventory and mapping of where all personal data is stored that includes cross-border data flows?	HIGH		
15	**Artificial Intelligence - Manages the risks and security implications of AI technologies while leveraging them for improved security outcomes**			
15.01	Does your software or platform include a Large Language Model (LLM)?	HIGH		
15.02	Does your software or platform include Natural Language Processing (NLP)?	HIGH		
15.03	Does your software or platform include Generative Artificial Intelligence (GenAI)?	HIGH		
15.04	Do you have AI's core technology and architecture?	HIGH		
15.05	Do you provide AI training, and what does your training require?	HIGH		
15.06	Do you ensure transparency in your AI processes, such as providing clear documentation or conducting regular audits? Please briefly explain.	HIGH		
15.07	Do you ensure data privacy and security in your AI components? Please briefly explain.	HIGH		
15.08	Do your AI components have protocols to mitigate or prevent bias from being introduced?	HIGH		
15.09	Do you have data privacy and security standards applied to your AI components?	HIGH		
15.10	Does your AI processes have models and protocols in place to ensure transparency?	HIGH		
15.11	Will the City of Raleigh data be used in training your AI models for use by other customers, and if so, how will you ensure the privacy and security of this data?	HIGH		
16	**Quantum Computing Readiness - Prepares for the potential impact of quantum computing on cryptographic systems and overall security practices**			
16.01	Does your organization have a Quantum Computing Readiness Plan that addresses issues such as moving to post-quantum cryptography or post-quantum software patches?	MEDIUM		