

## **ADDENDUM NO. 1**

**This addendum consists of 7 pages**

**TO:** All Plan Holders

**FROM:** Dan Castimore, IT Manager

**DATE:** January 5, 2024

**SUBJECT:** Answers to questions January 5th

**Bidders must acknowledge receipt of this Addendum in the appropriate place on the Bid Form. Failure to do so may result in the disqualification or rejection of the bid.**

Note: Information in this addendum takes precedence over original information. All other provisions of the document remain unchanged.

---

### **01-01 Plan Holder Question**

"Is vulnerability assessment and penetration testing of City's internal and external networks desired? If so, please approximate IP counts for the target networks."

*Response: This will depend on the selected proposal. The city has approximately 400 network devices.*

### **01-02 Plan Holder Question**

"Is this procurement from the internal audit department, IT department, or another office?"

*Response: The IT Department*

### **01-03 Plan Holder Question**

"Which operating system brands can be found in the IT environment?"

*Response: Windows and Windows Server are the primary OS brands. Limited Debian and Ubuntu servers.*

### **01-04 Plan Holder Question**

"Re: "Electronic submission: Details of electronic submission process will be provided in an addendum.", please provide these digital submission instructions."

*Response: See addendum #2 which will be issued concurrently with this addendum.*

### **01-05 Plan Holder Question**

"RFP page 7 defines deliverables 3.2 A, B, and C. Are these separate reports, or should we expect to prepare a single report?"

*Response: These should be 3 separate documents.*

**01-06 Plan Holder Question**

"What is the budget for this project?"

*Response: This project is funded with a \$35,000 grant.*

**01-07 Plan Holder Question**

"What is the budget for this project?"

*Response: See response to 01-07*

**01-08 Plan Holder Question**

"How many policies | procedures are currently in place?"

*Response: Approximately 10*

**01-09 Plan Holder Question**

"Have you had an information security risk assessment done in the past? Was in a Quantitative or Qualitative Assessment?"

*Response: an assessment was conducted in 2020. Unknown what type of assessment.*

**01-10 Plan Holder Question**

"Is there a rough budget for this project, so that we can tailor our proposal to that budget?"

*Response: See response to 01-07*

**01-11 Plan Holder Question**

"Do you have any information security staff on staff?"

*Response: There are no dedicated IT Security Staff.*

**01-12 Plan Holder Question**

"How many IT staff does the city have?"

*Response: One full time and one part time.*

**01-13 Plan Holder Question**

"Do you require the entire assessment to be performed onsite or can it be performed remotely? If a hybrid, what requirements of this assessment require an onsite presence and what items can be performed remotely?"

*Response: There is no requirement for an onsite presence.*

#### **01-14 Plan Holder Question**

"Is your technology environment fully discoverable from a central location? (via Site to Site VPNs, MPLS, SDWAN, etc..)"

*Response: the majority of the network is discoverable from a central location.*

#### **01-15 Plan Holder Question**

"Do you allow configuration and device discovery by a installed software agent collector? (Namely: Rapid Fire Tools, Network Detective data collector)"

*Response: Assuming this is a question about whether the City would allow a contractor to install an agent to conduct this assessment, the City would likely allow this. The agent would need to be screened prior to approval.*

#### **01-16 Plan Holder Question**

"Can all locations be scanned (via network scanning tool) from a single location?"

*Response: See response 01-14*

#### **01-17 Plan Holder Question**

"Are global admin credentials available for scanning network?"

*Response: for the majority of devices, but not all devices.*

#### **01-18 Plan Holder Question**

"Does your organization have access to Domain Admin, Global Admin or Administrator credentials for each of your IT assets?"

*Response: for the majority of devices, but not all devices.*

#### **01-19 Plan Holder Question**

" How many Servers are in the environment? (Virtual, Physical, Cloud,)"

*Response: Approximately 60, most are virtual*

#### **01-20 Plan Holder Question**

" How many desktop/laptops in each environment?"

*Response: Approximately 200. Most of the computers are desktops, laptops are less than 10%.*

**01-21 Plan Holder Question**

"Is there a domain or any directory services for authentication? Please describe:"

*Response: Active Directory*

**01-22 Plan Holder Question**

"Are there any development environments for custom applications? Externally Facing?"

*Response: No*

**01-23 Plan Holder Question**

"Are there any environments that are not accessible remotely? Please explain:"

*Response: No*

**01-24 Plan Holder Question**

"What are the key applications that host data? Are they in-house or cloud hosted?"

*Response: For security reasons this question will only be discussed with the selected vendor. We have 5 applications that host data.*

**01-25 Plan Holder Question**

"Are there any API integrations (Azure/O365, etc.)?"

*Response: For security reasons this question will only be discussed with the selected vendor.*

**01-26 Plan Holder Question**

"Do you use VLAN segmentation in your environment?"

*Response: Yes*

**01-27 Plan Holder Question**

"Do you have an inventory of the Information technology devices in your environment?  
How often is the inventory updated?"

*Response: An inventory is maintained and updated regularly. It may not be complete.*

**01-28 Plan Holder Question**

"Do you maintain warranty coverage on your infrastructure devices?"

*Response: For security reasons this question will only be discussed with the selected vendor.*

**01-29 Plan Holder Question**

"Is your cybersecurity program aligned to a Security Framework or Standard?"

*Response: Not officially, the City has a preference for CIS.*

**01-30 Plan Holder Question**

"Will this assessment be used by one or more of the city's agency to align with your CJUIS requirement?"

*Response: No*

**01-31 Plan Holder Question**

"Will you require a HIPAA risk assessment in addition to the Cybersecurity assessment or do you envision these as components of the same assessment?"

*Response: HIPPA would be very limited in scope.*

**01-32 Plan Holder Question**

"Are you audited against a Security Framework or standard?"

*Response: see response 01-29*

**01-33 Plan Holder Question**

"Is there a person in the City that owns the Cybersecurity Program?"

*Response: The IT Manager*

**01-34 Plan Holder Question**

"Is the municipality subject to any regulatory framework? (CCPA, GDPR, ITAR, DFARS, CMMC, CJUIS, PCI, etc....)"

*Response: Unknown*

**01-35 Plan Holder Question**

"The RFP states: 'The City consists of a number of departments, each with unique requirements, ranging from a Police Department and Dispatch center to a Public Library. This requires compliance with a number of standards such as HIPPA, CJIS.' Does the City intend the assessment to include assessment of compliance with HIPAA and/or CJIS and/or other?"

*Response: This will not be a major component of this assessment.*

**01-36 Plan Holder Question**

" Does the City have a preference of framework to assess the City IT against (NIST, CIS, etc.)?"

*Response: see response 01-29*

#### **01-37 Plan Holder Question**

"The RFP states: "The City of Kenai consists of approximately 200 computers and 118 users across 9 facilities using various wide area network connections." What kind of computers does this refer to (laptops, desktops, tablets, etc.)? How many servers are in scope?"

*Response: See response 01-19*

#### **01-38 Plan Holder Question**

"Does the City desire a physical security assessment of facilities?"

*Response: This will not be a major component of this assessment.*

#### **01-39 Plan Holder Question**

"The RFP states: "Device level security including routers, switches, cameras, wireless equipment, printers, copiers." Could the City provide estimated #s of each type of device in use?

- # routers and type
- # switches and type
- # cameras and type
- # wireless devices and type
- # printers and type
- # copiers and type"

*Response: The city is a Cisco shop. We have 2 routers, approximately 45 switches, 34 WAPs, and approximately 10 voice gateways. There are approximately 90 cameras, primarily Axis. 16 Konica Minolta Bizhub copiers, and approximately 20 HP printers.*

#### **01-40 Plan Holder Question**

"Does the City have a documented disaster recovery plan?"

*Response: There is no formal plan at this time.*

#### **01-41 Plan Holder Question**

"What is the approximate number of IT policies/pages the City has in place?"

*Response: see response 01-08*

#### **01-42 Plan Holder Question**

"Has the City had a prior cybersecurity assessment performed? If so, when was the most recent assessment completed?"

*Response: see response 01-09*

**01-43 Plan Holder Question**

"Does the City have an expected budget amount that can be shared for the project?"

*Response: See response to 01-07*

**01-44 Plan Holder Question**

"Can work be performed remotely (onshore), or does work need to be completed onsite?"

*Response: see response 01-13*

**01-45 Plan Holder Question**

"Regarding Kenai's Cybersecurity Assessment, will the infrastructure, policies, and/or response plan in this cyber audit encompass or include:

- Radio systems?
- Police dispatch systems (PSAPs)?
- Call handling systems?
- Video camera systems?
- Digital evidence management systems?"

*Response: The City network doesn't include a Radio System, Police dispatch system, or Computer Aided Dispatch system. A camera system and digital evidence system are present.*

**Attachments:**

*Current Plan Holders List*

***End of Addendum 1***

Planholders List  
Project: 2023 Cybersecurity Assessment  
Date: January 5, 2024

Name	Company	Email	Phone
McKinley Brown	Alliant Group	<a href="mailto:proposals@alliantcybersecurity.com">proposals@alliantcybersecurity.com</a>	832.388-4162
Tiffany S. Garcia	CBIZ Risk & Advisory Services	<a href="mailto:Tiffany.Garcia@CBIZ.com">Tiffany.Garcia@CBIZ.com</a>	512.340.7423
Adele Fiala	Certus Cybersecurity	<a href="mailto:adele.fiala@certuscyber.com">adele.fiala@certuscyber.com</a>	650.200.0758
David Anderson	CLA (CliftonLarsonAllen LLP)	<a href="mailto:david.anderson@CLAconnect.com">david.anderson@CLAconnect.com</a>	612-376-4699
John Kelley	CyberForceQ	<a href="mailto:jkelly@cyberforceq.com">jkelly@cyberforceq.com</a>	586.907,9751
Susie Crisp	Enterprise Risk Management, Inc	<a href="mailto:scrisp@ermprotect.com">scrisp@ermprotect.com</a>	305.447.6750
Farryn Huffman	Fit Solutions	<a href="mailto:fhuffman@fitsolutions.biz">fhuffman@fitsolutions.biz</a>	858.879.0798
Leslie Lyons	Guidepost Solutions LLC	<a href="mailto:LLyons@guidepostsolutions.com">LLyons@guidepostsolutions.com</a>	510.250.6241
Ahmad Zoua	Guidepost Solutions LLC	<a href="mailto:azoua@guidepostsolutions.com">azoua@guidepostsolutions.com</a>	
Jonal Machos	Konica Minolta	<a href="mailto:jmachos@kmbs.konicaminolta.us">jmachos@kmbs.konicaminolta.us</a>	
Sherman Gong	Konica Minolta	<a href="mailto:sgong@allcovered.com">sgong@allcovered.com</a>	
Tim Ferons	Konica Minolta	<a href="mailto:tferons@kmbs.konicaminolta.us">tferons@kmbs.konicaminolta.us</a>	
Lisa Freitas	Moss Adams	<a href="mailto:Lisa.Freitas@mossadams.com">Lisa.Freitas@mossadams.com</a>	505.353.1550
Elizabeth Carter	Online Plans Reporter	<a href="mailto:agcplans@gmail.com">agcplans@gmail.com</a>	907.561-5354
PATRICK SWERE	Securance Consulting	<a href="mailto:contactus@securanceconsulting.com">contactus@securanceconsulting.com</a>	877-578-0215
Ken Herold	Solutions3	<a href="mailto:ken.herold@solutions3llc.com">ken.herold@solutions3llc.com</a>	201.725.6389
JAY PRASAD	Tech Brains Solutions Inc.	<a href="mailto:jay.prasad@techbrainscorp.com">jay.prasad@techbrainscorp.com</a>	732.952.0552
Rick Anderson	True North Consulting Group	<a href="mailto:rick.anderson@tncg.com">rick.anderson@tncg.com</a>	651.705.1249
Thaddeus Dickson	XPIO Health	<a href="mailto:thad@xpiohealth.com">thad@xpiohealth.com</a>	253-651-7482