KENTUCKY COMMUNITY AND TECHNICAL COLLEGE SYSTEM

REQUEST FOR PROPOSAL ADDENDUM

SOLICITAION NO.:	RFP-0322
ADDENDUM NO.:	1
RFP ISSUE DATE:	October 25, 2024
ADDENDUM DATE:	October 30, 2024
OPENING DATE:	**NOVEMBER 6, 2024, 4:00PM EST**

The following information is being provided in response to questions received for this RFP:

1) Is the current IRP written as a single overarching document you use or have an A/S400 / IBM I within your infrastructure?
   a) Yes, it is a single overarching document.

2) Are there different version (or appendices) for each campus?
   a) No, not at this time. However, KCTCS may want to pursue including appendices if colleges have unique environments that should be noted in the event of an incident.

3) Is the IRP written in an 'all hazards' approach?
   a) It is not, but this is the desired expectation with the requested RFP to make the current IRP more comprehensive. The current IRP addresses more technical cybersecurity incidents including (for example) ransomware, malware, and operational disruptions such as DDOS and power/equipment failures.
   b) Other areas of interest that would be desired include:
   Physical Security Threats (break-ins, power outages, natural disasters)
   Third Party Disruptions (supply chain issues)
   Human-Caused Threats (insider threats, social engineering, human error)
   c) It is KCTCS' intention with this RFP that Offerors responding with a proposal would be able to help better determine what additional categories should be included.

4) Can you share the IRP table of contents or discuss what is currently included in the IRP, such as response to cyber, natural disasters, violent incidents, et cetera?
   a) Yes, please see below:

   Table of Contents

   1. Incident Response Contacts / Key Stakeholders
   2. Report and Identify Incident Type
      a. Malware, Ransomware, Phishing, DDOS, power/equipment failure, etc.
   3. Respond to the Incident
   4. Contain the Incident
   5. Recovery
   6. Lessons Learned / Post Mortem
      a. Work with affected College to understand how to prevent incident moving forward
   7. Responsible Party / IRP Initiator Information
      a. Who detected the incident
      b. Document findings

5) The following statement in section 3 is revised as follows:
   a) KCTCS is seeking proposals from qualified ~~full-service marketing agencies~~ companies to partner with KCTCS in providing review, assessment, and recommendations to KCTCS' Incident Response Plan.

6) Section 8. **SCHEDULE OF EVENTS** is revised as follows:

Issue date for RFP	**10/25/~~25~~ 24**
Deadline for Written Questions (Section 19)	**10/29/~~25~~ 24**
RFP Due Date	**11/6/~~25~~ 24**
Offeror Presentations (Section 9)	***To be Scheduled if needed.**

7) Is this an incident response plan for the KCTCS system as a whole?
   a) Yes, this is an incident response plan for KCTCS system as a whole
      i) Is this an individual incident response plan for each college?
         (1) No, this is an overarching IRP that will cover all 16 colleges

8) What are the key drivers behind this RFP?
   a) Minimize Damage and Loss
      i) Reduce the impact of an incident on operations, finances, and reputation.
   b) Ensure Timely Detection and Response
      i) Detect, contain, and remediate threats as quickly as possible.
   c) Protect Sensitive Data and Privacy
      i) Safeguard sensitive information (e.g., personal data, financial records, intellectual property).
   d) Regulatory and Compliance Requirements
      i) Meet legal and regulatory obligations regarding data security and incident management.
   e) Improve Organizational Preparedness and Resilience
      i) Establish a security-conscious culture and resilience against future attacks.
   f) Cost Savings and Resource Efficiency
      i) Minimize the costs associated with an incident, including response and recovery.
   g) Post-Incident Learning and Continuous Improvement
      i) Learn from each incident and strengthen security measures.

9) Has the current incident response plan been tested?
   a) Yes
      i) Has KCTCS done a tabletop exercise?
         (1) Yes, but not using the current IRP. KCTCS has participated in general tabletop exercises which served to help provide guidance for developing the current IRP.
         (2) What were the key findings?
            (a) The tabletop exercises identified potential gaps/incident types that the current IRP did not address

10) What is the expected growth in the next 3-5 years for KCTCS?
   a) KCTCS does not have this information available.
      i) Are there any plans to add additional colleges?
         (1) Refer to responses to questions 1 & 2.
   b) Do you use any 3rd party security providers, if so please elaborate.
      i) KCTCS works with select third-party providers across several areas, including data and network / security, SaaS / PaaS solutions, to reinforce our security posture. These partnerships enable us to enhance capabilities in threat intelligence, monitoring, and incident response, supporting our commitment to strong security and regulatory compliance. Each provider is carefully evaluated to ensure alignment with our security, privacy, and operational standards.
   c) How many full-time staff users?
      i) The information requested is not applicable to the scope of work for this RFP.
   d) How many staff members are there at each of the 16 colleges?
      i) The information requested is not applicable to the scope of work for this RFP.

11) Current Challenges: What are the primary challenges you currently face with your incident response process, and how do you envision overcoming these with a new plan?
   a) Current challenges involve addressing gaps in the current plan: Alignment with NIST standards, expanding on various types of modern-day attacks (physical, social engineering, technical, etc.), addressing technical resources available for handling an incident, etc. The overall goal is to develop an overall robust and more comprehensive IRP tailored to industry standards.

12) Service Options: We offer a variety of options and tools within our services that can help secure organizations like KCTCS. To provide a more relevant proposal, could you specify the number of licenses you anticipate needing?
    a) N/A. Licensing is not necessary. This RFP is intended for a single, one-time engagement to fulfill the specified scope of work. There is no expectation of a continuous or recurring arrangement following the completion of this project.

13) Budget Constraints: Is there a budget range for this project that you can share? Understanding this will help us align our proposal accordingly.
    a) The information requested is not available at this time. Please propose the best value your firm has to offer.

14) Timeline for Implementation: What is the anticipated timeline for the selection process and the implementation of the Incident Response Plan?
    a) Please refer to RFP Section 21. TERM OF CONTRACT.

15) Evaluation Criteria: What specific criteria will you use to evaluate the proposals? Are there any aspects that are particularly important to your organization?
    a) Please refer to RFP Section 25. EVALUATION OF PROPOSALS.

16) Do you expect an extension to the proposal date of 11/6?
    a) An extension on the proposal due date is not expected.

Bidders must acknowledge receipt of this and any addenda either with solicitation or by separate letter or email prior to award of contract. If by separate letter, the following information should be placed in the lower left-hand corner of the envelope:

RFP No.: RFP-0322
Title: Incident Response Plan

Name of Firm: _____

Authorized Signature: _____