MILWAUKEE TRANSPORT SERVICES, INC.

Friday, April 20, 2018

ADDENDUM NO: 1

RFP NO: MM-03-18 THREAT & VULNERABILITY ASSESSMENT

OPENING DATE: MAY 22, 2018 @ 2:00 PM, CST

PLEASE NOT THE FOLLOWING QUESTION(S):

Question: Given that assessing physical security and cyber security are different practices requiring different knowledge, skills and tools would MTS consider proposals which address either the Physical Security Scope or the Cyber Scope?

Answer: Please see section of the document where it states "Contract Term" (Page 4?)
It is the intent of MCTS to make an award in aggregate, however MCTS reserves the right to issue more than one PO if one vendor performs the threat assessment and another performs the penetration/vulnerability testing.

Vendors could collaborate with a company to submit one proposal with one of them listed as the prime.

Question: In the RFP Project Objectives, it states that MTS is seeking a Board-Certified organization. What are the acceptable Board Certifications?

Answer: MCTS would prefer that persons performing or involved in creation of the assessment are board certified. For the physical security assessment, ASIS International Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification or Certified Homeland Security Protection Professional (CHPP).

For the cyber assessment, the CISSP - Certified Information Systems Security Professional CISM, Certified Information Security Manager, CompTIA Security+ and CEH; Certified Ethical Hacker are all acceptable.

Vendors should base their estimates on the information provided on Page 12 of the RFP.

- There are approximately 800 wired / 1600 wireless / 825 cellular devices presenting more than 3200 IP addresses in a range of 331480 possible addresses
- The IT department manages and supports over 17 different hardware asset categories representing more than 2400 pieces of hardware
- The IT department manages and supports over 40 different software asset categories representing more than 589 software licenses
- The IT department currently operates 138 Windows and Linux based servers. Approximately 90 of these are virtual servers.
- There are 7 physical sites in our network

Question: Will the Penetration Testing scope include a cloud environment?

Answer: Only the MTCS network no hosted vendors. Please see Section in RFP labeled "MCTS Information Technology Network"

Question: How many total IP addresses (physical server or virtual server) are being tested? How many internal IP addresses? How many external IP addresses?

Answer: Please see Section in RFP labeled "MCTS Information Technology Network"

Question: How many web applications are being assessed?
Answer: No public facing websites are included.

Question: How many wireless networks are in place?

Answer: Please see Section in RFP labeled "MCTS Information Technology Network" for number of wireless devices. There is WIFI connected to our networks but if you are asking about physical locations the WIFI can be accessed from there are 7 properties and 408 buses.

Question: Will the Penetration Testing scope include social engineering (Phishing and/or Vishing)?

Answer: Yes

Question: For the physical penetration test, how many locations are being assessed?

Answer: The building locations are listed on page 12 of the RFP

Sign and return with proposal: _____