MILWAUKEE TRANSPORT SERVICES, INC.

Friday, May 4, 2018

ADDENDUM NO: 3

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

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

PLEASE NOTE THE FOLLOWING QUESTION(S):

Question: where can I find the information on the grant that is funding this project?

Answer: This is a 2017 Transit Security Grant

https://www.fema.gov/preparedness-non-disaster-grants

1) Has Milwaukee Transport Services, Inc. (MTS) previously conducted a Preliminary Hazard Analysis? Yes
    a. If yes, will the selected consultant have access to this document? Yes
2) Has MTS previously conducted Threat and Vulnerability Assessment? Yes, conducted by TSA surface inspectors through a pilot program.
    a. If yes, when was the last TVA conducted? 2011
    b. Will the selected consultant have access to these documents? Yes
3) Will the consultant have access to the full list of security incidents previously occurred at MTS? Yes
4) Will MTS would like a full or partial Blast Analysis conducted as part of the study? No
5) Will MTS designate a manager for this project? Yes
6) Is there a current inventory list of security physical and technological systems deployed at MTS? Yes
7) Could you clarify whether you want a VSS assessment done as part of this contract, and what exactly that scope entails? At the pre-proposal conference, MTS mentioned a camera RFP was issued last year, but the work is not complete. Page 9 of the RFP states: Evaluate the effectiveness and appropriateness of current security systems to include access control, intrusion detection, video surveillance, and lock and key control.
8) Can bidders submit a proposal as a Prime contractor, and also a separate proposal(s) as a sub or DBE sub on another team(s)? This answer is in Addendum 1.
9) Can we submit electronic copies on a CD instead of a USB? No.
10) Does your transit agency have its own police department? No
11) Does your transit agency have its own security department? Yes – The oversight of security is under the Safety, Security and Risk Management department.
    a. If security is used, is it contract or in-house? Contract
    b. If contract, are there metrics for the contract? Yes

12) How are problems on a bus handled today? Through the deployment of Transit security and the law enforcement support of 19 municipal and 2 university police departments.

13) Does your transit agency have a central location (command center) where all video or bus information is available? MCTS has a Transportation dispatch office for bus information. There isn't a Security Command Center but all video can be accessed centrally.

Is MCTS looking for a Phase approach to the results since a lot or not can change in a year, IT physical/Asset/Personal & Staffing? Please see page 10 of the RFP, section 2, #4 Your report must contain: *A capital improvement security master plan including implementation phases and estimated physical security upgrade costs.*

Does MCTS want us to propose the schedule of events? Yes, provide a schedule associated with milestone payments

In regards to analysis of the bus fleet, Is the AVL, Cameras, and alarms hardware in scope? Only as it relates to the ability to provide necessary safety for operators and passengers.

Are the Paratransit vehicles in scope as it was stated those were outsourced? Paratransit service and Vehicles are not included in this assessment

Will MCTS provide a complete and detailed inventory to check or is MCTS looking for the assessment to include discovery? An inventory of Security technology assets and floor plans will be provided

Regarding Wifi assessment- Is MCTS looking for the assessment to include an active hacking attempt(s) as well? Please follow the Cyber Scope information provided on page 9 of the RFP.

Would MCTS like the RFP cut up into sections? (With cost) to better aggregate the choices? The more detailed the pricing, the better.

Clarification needed:

In the RFP under "Written Report 2" it reads as follows: Prior to submitting a final written report and thirty (60) days prior to the submission of a final Written Report deadline, the consultant must submit a **Draft Report** to MTS for review and comments. 30 days

Is MCTS looking for the draft report to be provided 30 or 60 days prior to the submission? 30 days

Physical Security

Some questions called out a physical pen test. Is that the intent, as opposed to an assessment? If so, are there armed guards or transit authority police in these locations? Will they participate in the pen test? All references to penetration/vulnerability tests relate to the IT Network ONLY.

Item #3. How many institutional relationships related to crime prevention and emergency response exist today? The county of Milwaukee has 19 municipalities all with varying police, fire and emergency management personnel. There are 7 police districts in the city of Milwaukee who operate as a pseudo-independent municipality. There are 3 major universities that MCTS services, (two with independent police forces) and one technical college with multiple campuses. MCTS also operates in multiple cities in Ozaukee and Waukesha county. Other partnerships include Intelligence fusion centers. Emergency management offices, the coast guard, FBI, DHS, TSA and other partners.

Item #4. Approximately how many incident reports exist for the previous two years? All information from the last two years are contained in two excel documents and analyzed by type, time, severity and route.

Item #5. How many disparate systems exist for the systems in scope for this assessment? Unsure if this question references physical security or Cyber. Physical security systems include video, intrusion detection and access control. Cyber should reference the scope listed on page 12 of the RFP

Item #7. Approximately how many policies and procedures will be under review? As required by DHS to qualify for transit security grants, MCTS must maintain and update a System Security and Emergency response plan, a Continuity of Operations Plan, a Critical Incident Management Team Plan, a Sensitive Security Information Plan, and a Regional Transit Security Strategy. Other related employee manuals will also be available for review.

Cyber Security

Item #2. Of the 589 software license, how many serve business critical needs? All of this information is contained in our COOP plan. Will those be identified? Yes, to the successful proposer.

1. RFP states, "Physical security assessment with site visits and interviews. Consultants must list estimated number of site visits and assume 20 staff interviews."
    a. It is assumed that physical security assessment services will be provided via site walkthroughs and meetings, however, could some interviews/meetings be conducted via teleconference/Skype meeting if necessary? Please indicate how all meetings will be conducted and what employee interviews you will conduct – management, supervisors, mechanics, bus operators. Depending on the employee type, they might not have phone access. MCTS Employees do not have access to Skype.
2. RFP states "Include sample report(s), outlining issues considered, as well as a list of previous experiences and assignments."
    a. Due to project sensitivity, can a table of contents, list of issues considered, previous experiences and assignments be provided instead of a full sample report? Yes. The more detail you provide will give evaluators a better picture of the quality of work you provide.
3. RFP states "Provide your firm's approach to developing a quantitative, risk probability, frequency and event impact report. Include information that comprises the scores and losses considered."
    a. Does a full scoring list (i.e. excel spreadsheet, table, etc.) need to be provided, or can a written explanation/narrative of the information scoring be provided? The more detail you provide will give evaluators a better picture of the quality of work you provide.
4. Will more consideration (higher score) be given to a team that offers both the physical and cyber assessment services as opposed to one or the other? No
    a. The Scoring Criteria lists the Penetration/Vulnerability Test as 20 possible points. If this service is not included will that result in a 0/20 score? That item will not be averaged into the score
5. In the Deliverables section of the RFP, it states, "Prior to submitting a final written report and **thirty (60)** days prior to the submission of a final Written Report."
    a. Is the report to be provided within 30 or 60 days? 30 Days.

6. The RFP states the following, “This TVA will also address threats and vulnerabilities and their effect on regional transit partners like Amtrak, Waukesha County Metro and Ozaukee County Transit.”
    a. Are additional sites other than the 5 listed on page 12 of the RFP required to be included in the assessment? No
7. Has a budget been established for this project? Can this be disclosed? MCTS does not disclose budget

1. Is this a scan/validate computerized penn test? Or is this a redhat penn test? Under Part 4 of your technical proposal, all proposers should detail their firm’s methods and approach to testing the MTS Network
2. How many live Ip’s do you have? All proposals should be based on data presented on page 12 of the RFP
3. Where is infrastructure hosted? Is it in a third party hosted environment? Locally hosted.
4. How many web apps included in penn test? Web applications are not included in the scope.
5. How do you monitor your ecosystem? Unsure of what is meant by ecosystem.
6. As testing is progressing, what is the communication structure through the process? Proposers should include their best practices and communication process in their responses.
7. If we find breaches, how do you want it communicated to you? Proposers should include their best practices and communication process in their responses.
8. Are you applying any threat intelligence today? Yes
9. How do you monitor deep and dark web today? Not applicable
10. Do you have a Security Information and Event Monitor (SIEM)? No
11. How many Regional Transit Partners will need to be included in the assessment? Only those listed in the RFP – Amtrak – Waukesha and Ozaukee
12. Under the Cyber Scope section item four references a potential work effort, excerpt… “possibly assist in the development of security policies and procedures”. Is this development effort in scope and should pricing to be included in the rfp response, if so, how many policies are in place today and when were they last reviewed and amended? After the assessment and in your final report, we request that the vendor make recommendations of specific policy and procedure implementations that are appropriate to our operating environment. The creation of policies and procedures would not be the responsibility of the vendor.

1. Is the IT organization centralized or decentralized? Centralized
2. When was your last project of this nature performed? Physical TVA – 2011
3. Are there documented policies, procedures, standards, and guidelines in place? If so, how many? MCTS maintains a System Security and Emergency response plan, a Continuity of Operations Plan, a Critical Incident Management Team Plan, a Sensitive Security Information

Plan, and a Regional Transit Security Strategy. Other related employee manuals will also be available for review.

4. Can MTS provide its budget for this project? MCTS does not disclose budget
5. Can MTS provide an estimate number of incident reports that have been documented over the past 2 years? All information from the last two years are contained in two excel documents and analyzed by type, time, severity and route.
6. For the external network vulnerability and penetration test, what is the approximate number of active IPs? All proposals should be based on data presented on page 12 of the RFP
7. For the internal network vulnerability and penetration test, what is the approximate number of active IPs? All proposals should be based on data presented on page 12 of the RFP
8. Is a detailed firewall configuration analysis in scope? If so, what is the number of firewalls? Are the firewalls in HA mode? Please follow the Cyber Scope information provided on page 9 of the RFP.
9. Is web application testing in scope? Only the MCTS network is listed in the scope. If so, what is the number of URLs to be tested? How many applications?
10. Is there a wireless network assessment in scope? If so, how many controllers? All proposals should be based on data presented on page 12 of the RFP
11. Is a detailed server configuration review in scope? Yes, as they relate to security If so, what versions of Windows and Linux operating systems do MTS servers maintain? Please follow the Cyber Scope information provided on page 9 of the RFP as well as the system description on Page 12.
12. Is a network device configuration review in scope? Yes, as they relate to security If so, how many routers and switches would MTS like assessed? Please follow the Cyber Scope information provided on page 9 of the RFP as well as the system description on Page 12.
13. For the social engineering assessment, what methods are preferred (phishing, pretexting, baiting, tailgating) and what is the number of targets for each desired method? Under Part 4 of your technical proposal, all proposers should detail their firm's methods and approach to testing the MTS Network.

RFP MM-03-18

Please sign and return one copy with the RFP Documents.

We acknowledge receipt of Addendum #3.

_____ _____

Name **Company Name**

_____ _____

Signature **Date**