(RFP) Design and Installation of a Real-Time Traffic and Weather Monitoring System at Military Access Control Points

Date: June 28, 2022

RFP Questions were submitted from potential proposers.

Question 1
Section Number: 4.3
Paragraph Number: 1
Page Number: 12
Text of passage being questioned: “All proposals must be submitted by July 14, 2022 no later than 8:00 PM EDT.”

Question: We respectfully request an extension to the RFP due date by two (2) weeks and propose a new RFP due date of July 31, 2022, 8:00pm Eastern Time.

Response: US Ignite will revise the RFP due date to Friday, July 29, 2022, 8:00pm Eastern Time.

Question 2
Section Number: 3.2.1
Paragraph Number: 3
Page Number: 5
Text of passage being questioned: “These post-processed metadata must be stored in a database server on Fort Carson accessible via the CBRS network described in sections 3.2.6-3.2.8.”

Question: How long does the solution need to a keep historic records of images gathered? Is there any data sovereignty on the images captured?

Response: Any captured image data will be retained for 45 days. Processed data that is not in the form of images will be archived and retained.

The images captured are subjected to the law and governance of the US and state of Colorado. It must also be in compliance with the cybersecurity rules and laws of the DoD. The metadata or extracted information cannot be shared or distributed without consent from the necessary stakeholders.

Question 3
Section Number: 3.2.1
Paragraph Number: 2
Page Number: 5
Text of passage being questioned: “The proposed solution must include a computer vision framework capable of classifying the lane queue and each vehicle in the field of view, as well as an analytical framework capable of performing data analysis based on those vehicle classifications to create metadata useful for lane management.”

Question: Is there any existing data, images, feeds from the location or similar location to train

computer vision models from or should submissions assume training would begin at the start of the commission date?

Response: The proposer should assume training data will be collected by the system being proposed.

Section Number: 3.2.10
Paragraph Number: 1
Page Number: 9
Text of passage being questioned: “The Proposer will be responsible for providing support during the Operational Period while the traffic and monitoring system will be providing data to the AI4TW project. This support would include addressing any functional issues that are encountered during normal operations.”

Question: Should proposals including training and enablement as part of the total services included on the RFP?

Response: Operational support and training should be included in the total services of the proposal.

Question 4
Section Number: 3.4

Page Number: 10

Submit an approved system implementation plan prior to installation, inclusive of planned network architecture and interfaces with existing systems; approval from Carson DPW; insurance and licensure documentation of staff involved with installation and implementation plan.

Question: Are there published rates or details on the types of insurance mandated, levels of coverage expected or anything else that is relevant?

Response: Limit of Insurance Coverage shall be at least:

1. Commercial General Liability (CGL):
    - Products and completed operations, property damage, bodily injury, and personal & advertising injury with limits no less than $1,000,000 per occurrence, and a general aggregate with a limit of no less than $2,000,000.

2. Automobile Liability:
    - Insurance Services will limit no less than $1,000,000 per accident for bodily injury and property damage.

3. Workers’ Compensation insurance: Employer’s Liability Insurance with a limit of no less than $1,000,000 per accident for bodily injury or disease.

4. Cyber Liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.