S²MARTS Project: Misty Night – 5G Threat Assessment & Warning (22-08)
Project TalX Question & Answer | Date: June 23, 2022

1. Question: **Are we focused primarily CONUS or OCONUS?**

Answer: This network may be either CONUS or OCONUS; both are equally important. The proposal should articulate one (or more) relevant networks on which the solution will be demonstrate. Showing relevance to DoD use cases should be the focus.

2. Question: **Are we primarily focused on CONUS-based use-cases?**

Answer: See answer to Question #1.

3. Question: **Are you interested in solution to provide capability to create secure connections over untrusted networks for data and voice transport?**

Answer: For the purposes of this OTA, the government is interested in satisfying the desired end-state and success criteria, as well as the specification and system attributes, outlined in section three (3) of the RFS.

4. Question: **Are you looking forward to a pure software solution, or a pure hardware solution?**

Answer: Hardware, software, or both. The Department of Defense (DoD) network operators need tools that provide insight into users on the 5G network and methods for maintaining security across the network.

5. Question: **Can you provide any guidance on primary threats CONUS and OCONUS that DoD is concerned about?**

Answer: Anomalous behaviors are intended to be any behavior concerns observed by the network specific to DoD and would be analogous to the network health status which a mobile network operator is concerned with monitoring. Behavior may include activities such as overt attempts by unauthorized users to gain access to the network; authorized users to gain access to restricted network services or elements; repeated or abnormal attempts to request services or subvert commands from the network, etc.

6. Question: **Do performer facilities need to have facilities that allow for work at the program classification level? Or is the classification requirement for performers needing to have the appropriate clearance to perform work at government/customer facilities during demos/testing/integration?**

Answer: Awardees/Prototype Level Performers are not required to possess an active facility clearance to perform in support of the subject project. Phase 1 and 2 may be conducted at any classification level, including unclassified. Performers interested in a Phase 3 award must obtain the appropriate clearance prior to the start of Phase 3.

7. Question: **For Misty Night, we are assuming we are not in control of the core OCONUS at first but joining a cellular network already deployed.**

Answer: The solution should assume the network is already deployed and the solution does not control the core. For these proposals, one may assume the device is an authorized UE on the network but otherwise has no ability to control network, change deployments, network configurations, or so forth. One is a device on the network. Solutions where the network core and/or network operator are working with the device should be directed to the Gray Summer RFS.

8. Question: **Is the RFS to be strictly bid as FFP? Since this is new R&D type of work, CPFF is usually preferred by contractors due to the risk.**

Answer: The Government intends to award one Other Transaction Agreement as a result of this RFS; however, more than one award may be made if determined to be in the Government's best interest. The government will consider and entertain any costing model chosen by the performer but will ultimately choose the pricing model which is in the best interest of the government.

9. Question: **Is there broader USG interest in Misty Night that you are aware of (e.g., beyond DoD)?**

Answer: Yes. The Department of Defense (DoD) network operators need tools that provide insight into users on the 5G network and methods for maintaining security across the network. As a part of the solution, DoD seeks to understand the threats and vulnerabilities that are introduced by 5G capabilities and methodologies to protect against those that would exploit them. The solution must be capable of operating on both 5G standalone (SA) and 5G non-standalone (NSA) networks; moreover, since the NSA architecture includes 4G/LTE system elements, this necessarily implies a requirement to operate on 4G networks, as well.

10. Question: **What is the total end state device count potential... how many software licenses/devices should we plan for in our solution and pricing?**

Answer: This varies depending on the network itself. The NOC/SOC for a network spanning a large geographic region would expect a different number of UEs than a network intended for a small expeditionary command post. The demonstration should identify a use case and illustrate with UE numbers (real as well as simulated) relevant to that use case.

11. Question: **Will all potential end user devices run iOS or Android?**

Answer: The envisioned solution shall be capable of running on a UE/device and support up to 3GPP Rel 16. Moreover, the application must operate in both Standalone (SA) and Non-Standalone (NSA) 5G network configurations as well as support features such as sidelink, non-3GPP access (e.g., WLAN/WIFI) and provide capabilities for when the device is operating 4G, LTE configurations, 3G, and some limited support for 2G.

12. Question: **Will the CONUS range have connection to the Internet?**

Answer: Yes.

13. Question: **Will the government participate in the ATO process, or in submitting the ATO package for approval?**

Answer: An ATO is not required for Phase 1 or 2. For successful solutions moving into Phase 3, the government will work with the performer to identify and support key actions, which can include an ATO.

1. Question: **Will there be a Mobile Device Manager (MDM) for the range?**

Answer: Yes.

2. Question: **With the boundaries of a network blurring, how far across the network is the solution expected to operate? Is assurance meant to be guaranteed over every hop from one point to the last?**

Answer: We envision a solution that possesses the capability to provide network operators insight into anomalous behavior on the network according to their unique geographic setting and mission needs. This information is intended to provide the operator with enough information to make decisions and take action to maintain security of the network of interest, regardless of how the network is bound or defined.