S²MARTS Project: Gray Summer - 5G Core Based Threat Identification and Warning (22-07)
Request For Solutions (RFS) Question & Answer | Date: June 23, 2022

1. Question: **The RFS asks for a solution that scans for anomalous activities (e.g. out of band) impacting performance, confidentiality, integrity, and availability of the 5g network and its components. Does this mean that the solution requires external spectrum monitoring gear to look for out of band emissions, or is it desired that the solution infer this out of band behavior from within the existing core via performance metrics?**

Answer: The solution does not require external spectrum management gear. The solution shall only monitor portions of the spectrum which are within the band(s) of interest. The solution will monitor, identify, and warn of jamming/unauthorized operations on such band(s) of interest.

2. Question: **Is there any interest in prototyping novel chip-scale front-end design? The final product will be packaged in PCB.**

Answer: A proposed solution would need to show how novel chip-scale front-end design meets the objectives laid out in the RFS.

3. Question: **Is the total funding available meant for all three phases or is additional funding anticipated to become available after Phases 1 and 2?**

Answer: The proposal and funding are meant for Phase-I and Phase-II. If the government proceeds with Phase-III, additional funding and details may be provided. The current and most important focus is on Phase-I and Phase-II.

4. Question: **There is mention in the RFS of a down select between phases 2 and 3. Is the proposal for this effort meant to cover all three phases or just up to the point of the down select?**

Answer: See answer to Question #3.

5. Question: **Proposal Structure and Assessment Methodology (p. 7): Given the potential phase 3 award date, how will this be executable? Will the Government amend this Phase 3 award date to a later date?**

Answer: Phase 3 awards will be determined at an appropriate time. Performance in Phases 1 and 2 will help determine whether Phase 3 is warranted.

6. Question: **Anticipated Number of Awards (p. 5): The Solicitation states: "Partial responses addressing only a subset of the project's overall objectives are not permitted for this effort." Could the Government specify which objectives are covered under this (specifications, prototype attributes, etc.)?**

Answer: The solution should meet the objectives listed in the RFS.

7. Question: **Would the DOD be willing to allow bidders to leverage their own 5G labs vs Idaho National Lab for prototype testing if they felt this would lead to a better overall solution?**

Answer: Proposers can use their own lab for development and testing. But the government will desire testing/demonstration to occur outside of the vendor's lab at later stages of capability maturity.

8. Question: **Is the govt looking for demonstration of what capabilities existing wireless service providers have related to Core Based Threat Identification and Warning?"**

Answer: The government seeks a solution that meets the objectives in the RFS, not a demonstration of existing capabilities. If a proposer believes existing capabilities fully meet the objectives, the proposer may offer that as a solution.

9. Question: **Is the govt looking for how such capabilities will be implemented in a govt owned and operated Wireless (4G/5G) network?**

Answer: This network may be either government or commercial; 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.

10. Question: **What needs to be demonstrated at the govt Idaho Lab? Please provide clarification.**

Answer: The performer will conduct a Demonstration of the prototype on a DoD selected range facility, during which the prototype's capabilities must be successfully demonstrated. Provide capability at the Core to reduce risk of information exploitation throughout the network. It should be assumed the Core and associated network are operated by a cooperative entity allowing for network appliance additions and modifications that do not otherwise negatively affect network performance or operations. In conjunction with the Network Management System, the requested prototype continually scans authorized network elements (servers, routers, controllers, base stations, UEs, etc.) for degraded services and anomalous behavior such as security breaches, unauthorized network access, equipment compromise, etc. Scan network for unauthorized network elements and provide capability to shut-down or isolate equipment. Provide a graphical user interface and security dashboard which displays the security posture of the network and alert anomalous behaviors that might compromise the security of the network to the operator. The dashboard should provide the operator with enough information pertinent to DoDs specified missions and provide insight to take actions in response to perceived threats.

11. Question: **Section C of the RFS mentions both "... Performers are not required to possess an active facility clearance" but "must state or demonstrate ... their ability to meet the facility/personnel security clearance requirements". Must the prime contractor themselves be required to do this, or can the classified facilities and personnel be entirely provided by a subcontractor?**

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.

12. Question: **RFS Reference: Section B, Sub-section 3 Question: Will our capabilities installed in the testbed have access to unencrypted control-plane and user-plane traffic?**

Answer: When installed in the testbed, the solution may assume it is the network operator and therefore has capabilities available to the network operator. For example, the network operator would have access to credentials/keys for any control plane traffic the network operator chooses to encrypt. Similarly, the network operator would have access to any credentials/keys it may use to encrypt user-plane traffic. The solution is run by the network operator and therefore has access to those same credentials/keys. However, the solution is responsible for determining how relevant encrypted data is delivered to the solution and how the corresponding credentials/key are managed by the solution. In other words, the solution may not simply assume that every control plane message and every key is provided to the solution. Note a UE may encrypt data using its own credentials/keys without the involvement or approval of the network operator. For example, a UE may run an app such as Signal, Messenger, WhatsApp, and so forth. This can result in user-plane traffic that cannot by decrypted by the network operator. Even if the network policy prohibits this type of encrypted traffic, the solution must assume UEs and/or compromised components may fail to follow network policies. In fact, one common purpose of a NOC/SOC is to identify actions that violate network policies.

13. Question: **RFS Reference: Section B, Sub-section 3 Question: Can the Government help bound the scope of UE scanning? (a) Can we assume that the UEs are under the control of the Government? (b) What OSs should be considered e.g. iOS, Android, Windows, Linux, etc.? (c) How many UEs should be considered?**

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.

14. Question: **RFS Reference: Section B, Sub-section 3, "Prototype Attributes", bullet 1, sub-bullet 1 Question: The RFS states "In conjunction with the Network Management System, the requested prototype continually scans authorized network elements..." What is an authorized network element? If the statement means that the prototype should scan only elements that the prototype or the user are authorized to scan, then what provides a determination for a network element being authorized or unauthorized to scan?**

Answer: The network policy determines what is an unauthorized element based on its behaviors. 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. The following examples are illustrative, not prescriptive and may not apply to your solution. An unauthorized element could be a UE that lacks the appropriate credentials, has its credentials expired, or has behaved in a way that should exclude it from the network. An unauthorized element could be a server attempting to act as part of the network MEC. An unauthorized element could be a router/switch/device that was not expected to be part of the core network or was incorrectly installed on the network. The NOC/SOC is intended to help network operators understand the threats present and provide actionable information. What the network operator believes/expects to be elements of the network may not always correspond to what elements are actually part of the network.

15. Question: **RFS Reference: Section B, Sub-section 3 Question: Should we plan to use existing compute, storage, and networking resources or should we provide our own? If the former, then can the Government provide resource limits per data center?**

Answer: The prototype should provide the resources necessary for the proposed solution.

16. Question: **RFS Reference: Section B, Sub-section 5 Project Deliverables Question: Can the Government specify the individuals or distribution list to submit electronic deliverables to?**

Answer: This will be addressed upon award(s).

17. Question: **RFS Reference: Section B, Sub-section 5 Project Deliverables Question: Shipping timelines are subject to external variables (supply chain, pandemic, natural disaster, etc) outside of the control of the Government and Contractor. In some cases, deliverables that are shipped may arrive during non-working times to Government sites or may be delayed/lost at no fault of the Government or Contractor. Can the Government specify how the delivery of physical deliverables will be evaluated for timely submission (date of shipping, window of receipt, etc.)?**

Answer: The proposal should clearly identify any supply chain risks and those will vary with the proposed solution. For example, a solution that is dependent upon procuring a specific piece of critical hardware has a different supply chain risk than a solution that is a pure software-based solution.

18. Question: **RFS Reference: Section E, Sub-section 5. Contents of Pricing Response Question: Can the Government specify whether all three phases of the RFS should be priced in the pricing response?**

Answer: Cost proposal should cover Phase 1 & 2.

19. Question: **RFS Reference: Section V, Sub-section 5. Project Deliverables Question: Can the Government confirm that Project Deliverable 8: Final Prototype Deliverable should only be delivered in Phase 3?**

Answer: Phase 2 will include a prototype demonstration and potential for a down select at month 12. During Phase 2, selected Awardees will begin the prototype production and test and evaluation process for transition.

20. Question: **RFS Reference: Section B, Sub-section 3, "Specifications", bullet 1 Question: The RFS states "The scope of required scanning... including but not limited to: peer-Core Networks (e.g. through roaming partners, Managed Virtual Network Operator (MVNO) relationships, etc.)" Are we to assume that these peer-Core Networks are also operated cooperatively allowing for network appliance additions and modifications, per RFS Section B, Sub-section 3, "Prototype Attributes", sentence 2 "It should be assumed the Core and associated network are operated by a cooperative entity allowing for network appliance additions and modifications..." If yes, then would remote access be granted into these peer networks?**

Answer: You should NOT assume a peer network allows network appliance additions and modifications. Proposals should assume the (home/primary/main) network is operated in a manner that allows for network appliance additions and modifications, but this does not necessarily extend to peers. For example, a peer network could be operated by the same entity, could be the network of a coalition partner, or commercial competitor. For example, a coalition partner may not be willing to add hardware and in some cases, it may not be in the government's interest to provide that hardware to a partner. It is not reasonable to assume the peer network would also support adding new appliances to their network. It is reasonable and appropriate to assume there is a decreased capability when a peer network limits what additions will be allowed.

21. Question: **RFS Reference: Section B, Sub-section 3 Question: What is the size and scope of the testbed to use for solutioning and pricing purposes? (a) Number of data centers and their use, e.g. mobile core, mobile edge, application servers, combination thereof, etc. (b) Number of physical servers, VMs, containers, NFs, and applications per data center? (c) Number of gNBs, eNBs, and UEs? (d) Hypervisor technology? (e) Is any part of the system under consideration hosted in a public cloud? (f) Is an IMS present? (g) Can the Government provide a real or notional diagram of the lab?**

Answer: This varies depending on the network itself. The NOC/SOC for a network spanning a large geographic region would comprise a greater physical and digital footprint than a network intended for a small expeditionary command post. The demonstration should identify a use case and illustrate with infrastructures (real as well as simulated) relevant to that use case.

22. Question: **RFS Reference: Section B, Sub-section 3 Questions: Can the Government describe the current RAN implementations and capabilities?**

Answer: There is no specific RAN implementation associated with this RFS. The solution should be designed to work in one or more 5G networks that could reasonably be considered relevant to DoD use cases. One should assume any RAN is compliant with 3GPP standards.

23. Question: **RFS Reference: Section B, Sub-section 3 Question: What capabilities exist in the testbed for solutioning and pricing purposes? Continuous monitoring of control-plane and user-plane traffic; zero trust features; traffic generation and test measurement equipment; log movement, aggregation, normalization, storage, and analysis; FW for metadata/events generation; etc.**

Answer: For budget and planning purposes, proposals should assume the range facility will be a DoD provided range at Idaho National Laboratory. Range facilities may vary and will be determined as part of an award.

24. Question: **RFS Reference: Instructions, 4. Contents of Response a. Compliance Question: The compliance section states, "In addition to the mandatory representation included as Attachment 1, respondents must include the following statement within the Compliance section (with the applicable answer checked):" Can the Government confirm that the referenced Attachment 1 is the solicitation file titled "Attachment-A_Mandatory-Section-889-Representation-1"? Can the Government provide instructions for completed Attachment 1 submission to indicate whether it can be a separate file from the Technical response volume, or whether it should be attached consecutively to the Technical response volume?**

Answer: Yes, it is. The document will need to be checked as to whether or not you will or will not provide covered telecommunications equipment or services and signed by the company. Yes, it can be provided as a separate attachment.

25. Question: **RFS Reference: Instructions, 3 Phased Approach Question: Can the Government clarify the places of performance for the work by phase?**

Answer: For budget and planning purposes, proposals should assume the range facility will be a DoD provided range at Idaho National Laboratory. Range facilities may vary and will be determined as part of an award.

26. Question: **RFS Reference: Instructions, C Question: The RFS states that key performer and sub performer personnel assigned work under the agreement shall at a minimum be U.S. citizens and have a valid TS/SCI clearance as required. Given that sub performers may provide commercial tools to the Key Performer for integration, the requirement for sub performers to have TS/SCI may limit the solution and may not benefit the Government. For example, a sub performer may only provide tools, equipment, or software for the performer to integrate into the full solution and will not need to access classified facilities and material in that transaction. Can the Government modify the security clearance requirement to require clearance requirements only for individuals who require access to classified materials and facilities?**

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.

27. Question: **RFS Reference: Instructions, 4.A Question: Are all prime contractors and their teammates required to submit Standard Form 328 (Certificate Pertaining to Foreign Interest) or is this form only necessary if the company has a FOCI to disclose?**

Answer: The Standard Form 328 is only necessary if the prime or subcontractor have FOCI to disclose.

28. Question: **RFS Reference: Instructions, C Question: Can the Government define the scope and type of NATO information access required?**

Answer: Please provide reference, do not see reference to NATO information in RFS, Section C.

29. Question: Can the government provide additional information on the dashboard information required for the DoDs specified mission?

Answer: The data display (data dashboard) must be relevant to the network use case and network objectives. For example, in some use cases the number of users on the network as well as related information on association attempts, invalid authentication, and so forth may be highly relevant. In other use cases, spectrum sharing behavior may be highly relevant. In yet another use, QoS factors such as latency, bandwidth, and jitter may be highly relevant. This information should be displayed in a way that is easily understood and actionable by a network operator. These are illustrative and not prescriptive examples. The proposal should clearly identify the data to be displayed, justify its relevance, and be adaptable. Applications must include a graphical user interface with control functions to allow both manual and automatic scanning and threat reporting. The dashboard should allow the network operator to customize the data displayed based on specific mission interests and location of mission operations.

30. Question: Is there only one award or will there be multiples with a down select? The solicitation describes both as possibilities.

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 also reserves the right to not select any of the solutions proposed.

31. Question: If there are multiple awards in each phase, can you provide ROM funding for each award?

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 also reserves the right to execute fewer awards than anticipated, select aspects of a proposal for award, or not select any of the solutions proposed. The Government will collaborate with prospective awardees prior to finalizing the award.

32. Question: Will the Phase 2 prototype be demonstrated in a classified environment?

Answer: 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.

33. Question: What facility clearance is required? The solicitation implies that a facility clearance is required but later states that the ability to receive, store, fabricate, modify, or generate classified information or material at the performer's own facility is not required.

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.