S²MARTS Project 20-03: Radio Frequency Spectrum Dominance

Request for Solutions (RFS) Questions & Answers | Posted June 4, 2020

1. **Question**: Section 6, number 2 in the RFS mentions a deliverable: \" A software tool that is capable of scraping the internet to detect threats to DoD interests abroad. Is this scraping tool mainly looking at internet traffic across the RF being monitored, or is this intended to be a separate analytic tool with the intent of gather intel from overall NIPRNET traffic? We are curious as to the RF relationship of scraping the internet for this deliverable.

   Response:
   Any internet tool would primarily be looking at internet traffic as it pertains to a communications path.

2. **Question**: Is it expected to correlate a scraped event from the internet to a particular RF event being sensed (is this the main intent of the scraping tool)?

   Response:
   The capability of the internet/Wi-Fi/IP traffic monitoring is dependent on the vendor solution.

3. **Question**: What is the scope of the term “scrape the internet” as the Government employs in Proj. Deliverable #2? Does scrape the internet only apply to active IP sessions that have an endpoint from within the previously identified operational zone of interest?

   Response:
   See response to question 1.

4. **Question**: The term scraping the internet – is it defined as the standard web-crawling, data parsing & extracting, data normalization, & data serialization/cataloging? (Ref Deliverables 6. 2.) Are there specific data types required for the internet scraping (social media, dark web content, Government Information networks)? (Ref Deliverables 6. 2)

   Response:
   See response to question 1.

5. **Question**: We have a high-speed, low-SWaP RF sensor that may be helpful here, but I’d like to better understand the relative importance of RF sensing vs internet scraping, to paraphrase the solicitation. Can you provide some guidance on how you see those two modalities working together and what their relative priorities are? What is meant by internet scraping?

   Response
   The internet RF spectrum is only one portion of the desired signals of interest.

See response to question 3

6. **Question**: Please confirm that scraping the internet signals should be only off the air (4G/5G/Wi-Fi) and not wired.

   Response
   This is correct. IP traffic would be limited to 4G/5G/Wi-fi-type signals.

   See response to question 3

7. **Question**: Is the desired system SWAP-C constrained? If so, what are the SWAP-C constraints? What SwAP and Packaging is required/desired for the Prototype? Rack? Transit Case? Manpack?

   Response
   The solution must conform to transport by a military helicopter.

8. **Question**: Are the RF systems intended to be collected in the field or in a laboratory environment? If in the field, should it operate from a mobile, portable, and/or low-SWaP platform?

   Response
   See response to question 7, 34

9. **Question**: Is there a Size, Weight and Power (SWaP) and operational time and life requirement? What is the operational use case: Fully autonomous, semi-autonomous, or human directed? How desirable is a low-SWaP application?

   Response
   There is no specification for operation to autonomous, semi-autonomous, or human directed.

   Low-SWaP is desirable.

   See response to question 34

10. **Question**: Are there strict requirements on operational processing latency: threats identified sub second (munitions), seconds (alerts), minutes (thorough threat vetting), hours (tactical, strategic)?

    Response
    No latency requirements have been specified. The system is intended to operate in real time.

11. **Question**: What are the typical assets to protect? Are these only fixed bases and underway maritime vessels as indicated in Paragraph 4.

    Response
    See response to question 34

12. **Question**: Sect. 5 1st Paragraph, "seeks a capability to detect and counter emerging threats…" Should the proposed solution also defeat/jam/spoofing/ DF/block the threat? Should it locate it? Is it required to ignore legitimate signals? Legitimate content transfer?

    Response
    There is no requirement to defeat/jam/spoofing. The desire of the RF detection system is to detect and identify these types of activities. Vendors may propose concepts to ignore legitimate signals and legitimate content transfer.

13. **Question**: Does the scope of the software tool include monitoring IP packets that are transmitted or received by DoD devices?

    Response
    DoD devices have not been specified as target platforms.

14. **Question**: Will such a software tool need inter-node communication capabilities across a number of in-field devices? Or, would stand-alone, on-device functionality suffice for this RFS?

    Response
    The vendor solution will determine the requirement for stand-alone or multi-device functionality.

15. **Question**: Would such a tool be deployed in static locations or need to incorporate mobility in its design?

    Response
    The solution is desired to be static at a fixed location.

    See response to question 34

16. **Question**: What are the computational resources available for deployed, in-the-field systems? Would embedded edge GPU/Tensor devices be open for consideration?

    Response
    The vendor is responsible for proposing computational and/or hardware requirements for the implementation of their solution.

17. **Question**: Should the software tool learn the network health and baseline *a posteriori*, through interaction with the environment? Or, should the system incorporate some pre-defined baseline, perhaps as a function of locale or region?

    Response
    The vendor is responsible for proposing a solution to provide baseline assessments.

    See response to question 9.

18. **Question**: Does the scope of the software tool include monitoring the internet at large such as websites, social media, search engines, and dark web to detect threats?

    Response
    See response to question 4.

19. **Question**: Should the software tool search the internet for possible threats against specific DoD assets, for example searching for threats against "XYZ forward-operating base" or possible codenames for this asset?

    Response
    This function has not been specified. Vendors may propose any unique solution to address the problem.

20. **Question**: Should the system attempt to break enemy encryption? If so, what types of enemy encryption schemes should the software tool attempt to decrypt in order to monitor traffic?

    Response
    There is no requirement to break encryption.

21. **Question**: What languages, beyond English as the primary reference language, should the system expect to encounter? If so, what are the target languages?

    Response
    RF signals of interest are the target independent of languages.

22. **Question**: Should flagged material or conversations be processed, beyond for example, high-level flagging of named DoD assets or overt threats? For example, would a sentiment value, conversation tracing, or agent tracking or identification, etc., be desirable features in the final solution?

    Response
    Exploitation of the signal traffic is not a requirement. Vendors may propose any unique solution to address the problem.

23. **Question**: Should the system consider flagged conversation tracking over time? If so, to what degree?

    Response
    See response to question 22.

24. **Question**: For material assets, will the system have access to an inventory database? If so, would this be within scope for system development and use as a reference? What level of detail can be expected?

    Response
    Please submit more information for an accurate response.

25. **Question**: More generally, what "learnable" data would be made available? If higher-degree contextual processing of foreign internet conversations is desired, ability for our models to learn the deeper

language contexts, e.g. use-cases, technical contexts, etc., would greatly aid in identifying and flagging threats beyond rudimentary named-entity identification.

Response
RF datasets could be made available dependent upon the vendors requirements and applicability.

26. Question: Is it reasonable to assume that the final system will be deployed in a datacenter with standard computational resources, including availability of GPUs for accelerated processing?

Response
See response to question 34.

27. Question: Will such systems need to be ported to field applications (as part of this RFS) that may include limited computational resources?

Response
The vendor must provide computational platforms required for the solution.

28. Question: Should the virtual database incorporate or organize data external to a team's solutions and efforts? If so, what is the scale of the amount of data? How many disparate data stores?

Response
A virtual database has not been specified. Vendors may propose any unique solution to address the problem.

29. Question: Is there a clear definition of a virtual database? (Ref Deliverables 6. 3.)

Response
See response to question 28.

30. Question: Is there an expected location for Phase III CONUS or OCONUS field testing that can be used for cost estimates?

Response
OCONUS field testing site has not been specified, however the location would be within the CENTCOM AOR.

31. Question: Is there a preferred means for alert delivery outside of the dashboard application being used by the system operator?

Response
An alert delivery has not been specified. Vendors may propose any unique solution to address the problem.

32. Question: Is the system intended to interface with or be integrated in other Navy or DoD platforms?

Response

There is no requirement for interoperability with any specified Navy or DoD platform.

33. Question: Will this hardware be installed on any platforms, for example, aircraft, ships, vehicles?

Response
The solutions for Phase III will be evaluated at a fixed facility.

See response to question 34

34. Question: Please indicate the platform of the required solution?
a. Is it naval/fixed land based/vehicular/airborne/back office?
b. For land-based solutions: should they be optimized for rural/urban/sub-urban?
c. Should the prototype meet military environmental conditions? Should the final product meet them? Would IP67 be sufficient?

Response
The solutions for Phase III will be evaluated at a fixed facility.

The system should be configured for urban environments.

There is no requirement to meet full military environmental specifications. Ruggedized commercial standards may be acceptable.

35. Question: Are there any form factor, size, weight, power, or cost requirements for the desired system?

Response
See response to question 7.

36. Question: What is the required refresh rate for information provided to the system operator?

Response
See response to question 10.

37. Question: Does the Navy have a target annual expenditure for maintenance following system delivery in a follow-on contract?

Response
There is no specified annual expenditure ceiling for follow-on maintenance and support.

38. Question: What are the criteria for determining if a signal is anomalous? In what ways are signals dangerous versus innocuous? Is this based on the content of the message, or the RF characteristics?

Response
Vendors may propose any unique solution to address the problem.

39. **Question**: Is the RF analysis and anomaly detection performed in real-time? If latency an RFSD performance metric? Are signals associated with an emitter via the baseline? Is there a need to analyze and identify anomalous emitter behavior?

    Response
    See response to question 10 and 12.

40. **Question**: When monitoring 4G/5G/Wi-Fi spectrum, should the system learn the baseline spectrum behavior and then detect anomalous behavior? For example, should the system continuously learn what normal LTE spectrum looks like in this geographical area and then identify when the LTE spectrum differs from normal?
    Response
    See response to question 12.

41. **Question**: Should the system estimate the geographical location of the anomalous transmission? If so, to what degree of accuracy and precision?

    Response
    See response to question 12.

42. **Question**: Please define how fast the system should produce an automated notification of an anomalous signal once detected

    Response
    See response to question 10.

43. **Question**: Does the Government intend Project Deliverable 1 to require the proposed solution to perform an analysis of collected spectrum data only at Layer 1 of the OSI model? Does the Government intend there to be a baseline requirement to collect and analyze data on spectrum communications at Layers 2-7?

    Response
    The project deliverable 1 should be capable of performing the proposed solution against representative signals in a representative environment.

44. **Question**: Should the system estimate the identity of the transmitter? If so, to what degree of detail? For example, just enemy/friendly or more detailed such as username, user affiliation, hardware make/model, MAC address, wireless standard, modulation/coding scheme, etc.?

    Response
    All signals of interest should be identified. Vendors may propose any unique solution to address the problem.

45. **Question**: Can you clarify the connection between the collection and identification of anomalous RF signals, and the need for trusted microelectronics in the supply chain? Is the software tool for scraping the internet to detect threats intended to access the internet through the RF signals obtained by the RF spectrum analysis tool?

Response
The RF Spectrum analysis tool or system must be capable of collecting and analyzing radio frequency and other spectrum communications. Vendors may propose any unique solution to address the problem.

Vendors are expected to comply with DoD standards for RF devices and trusted microelectronics compliance.

46. Question: Can you clarify what is meant by anomalous signals?
a. Does the desired system need to examine the information content of signals?
b. Does the desired system need to determine the location of emitters in the environment?

Response
See response to question 12 and 44.

47. Question: In what environment will this system payload perform its functions? Or what platform will the system reside on i.e. sea, airborne (what altitudes), ground?

Response
See response to question 34.

48. Question: What are the environmental requirements for the RFSD system? What conditions must the system be capable of operating in?

Response
See response to question 34.

49. Question: Does the Government intend Project Deliverable #3 to require the proposed solution such that physical instance of the database is not present in the operational area?

Response
There is no specification for this capability. However, vendors may propose any unique solution to address the problem.

50. Question: The deliverable table says nothing about Phase 3. Please update the deliverable table to include Phase 3.

Response
The deliverable for Phase 3 is a Military Utility Assessment, extended user evaluations, in theater training, and technical reports. The deliverable table identifies by phase each deliverable.

51. Question: What is the operational CONOP for the prototype system? This question seeks the basic assumptions for system design such as availability of power, cooling, use of operator positions and monitors, desired monitoring range, need for antennas, etc.

Response

Vendors can assume 115V AC power is available to support any proposed solutions. Vendors may propose any unique solution to address the problem.

52. Question: Is there interest in going above 6 GHz for RF signal collection and analysis?

Response
The requirement for signal collection and analysis is 40 MHz to 6 GHz. However, vendors may propose any unique solution to address the problem.

See response to question 74.

53. Question: Is direction finding a requirement for the RFSD system?

Response
Direction finding is not a requirement, however geolocation of signals and sources is required.

See response to question 12.

54. Question: Is the RF system purely passive (receive only)? Or is it acceptable to add active (transmitting) items for better performance?

Response
Vendors may propose any unique solution to address the problem.

See response to question 12 and 22.

55. Question: If multiple Phase 1 awards are made, does the Government plan to downselect for Phase 2 awards, and subsequently for Phase 3 award?

Response
There is a potential for a downselect, any for any, all, or no vendors to be funded and permitted to proceed to each subsequent phase depending on solutions provided.

56. Question: What is the size of the unit? Is it for a man portable vehicle like a tank, Humvee, and/or drones?

Response
See response to question 7 and 34.

57. Question: Is DC power available?

Response
See response to question 51.

58. Question: Is LCD display part of the unit or will it connect to laptop computer or iPad?

Response
Vendors may propose any unique solution to address the problem.

59. **Question**: Given the spectrum of RF signal collection, what is the anticipated rate and volume of data collection for the duration of a mission?

    Response
    The vendor solution or collection capability will determine the volume of data collected during the mission.

60. **Question**: Will collected and/or uploaded data be separated into multiple classification levels within the on-board storage system/mission computer?

    Response
    There is no requirement to separate data into multiple classification levels.

61. **Question**: What is the objective size of the overall system?

    Response
    See response to question 7.

62. **Question**: Page 2, Section 5 stated compare them against a baseline. Would you clarify is this a baseline to be provided by the Government?

    Response
    The vendor solution must be capable of establishing any required baselines. Vendors may propose any unique solution to address the problem.

    See response to question 17.

63. **Question**: Page 4, Section 6, item 2: for OCONUS deployment, to scrape the Internet will language translation be required?

    Response
    See response to question 21.

64. **Question**: Is the period of each phase intended to be 12 months? What are the timelines required for each phase?

    Response
    The period of each phase is dependent on vendors solution and performance.

65. **Question**: How important is user-friendliness at the end of each phase? What minimum metadata should be provided to the user about a detected anomaly? For example, transmitter type, wireless standard, and likely user identity? Anything other info?

Response
See response to question 31.

66. **Question**: What is the intended RX form factor: long term/short term fixed field deployment (power grid or battery), semi-fixed command center, or mobile deployment mounted/dismounted) hand-held, man-pack, UAV?

Response
See response to question 7 and 34.

67. **Question**: What is the TRL requirement for the prototype?

Response
The TRL is dependent on the vendor's project development.

68. **Question**: What is the minimum anomaly detection rate required?

Response
See response to question 10.

69. **Question**: RFS - Page 5: Deliverables. What is the difference between the Technical Report and Final Technical Report? They appear to be redundant as it relates to reporting following each phase. Please clarify.

Response
Please see Q&A posted for the Project TALX conducted for this project.

70. **Question**: What is the current technology being used by the customer/end user?

Response
RF spectrum analysis tools are being used.

71. **Question**: Who is the customer of this effort and who is the target end user? Is it for special forces, small combat units, large combat units, intelligence agencies etc? What is the target of interest for the prototype?

Response
USCENTCOM is the intended customer.

See response to question 34.

72. **Question**: Is machine learning detection and classification algorithm development in scope for identifying threats or is hardware the main focus?

Response
Vendors may propose any unique solution to address the problem.

73. Question: Is there a real-time computing platform that this solution would need to integrate with?

Response
See response to question 27.

74. Question: What bandwidth are you interested in, and are there particular frequency bands of interest?

Response
See response to question 75.

75. Question: Sect 5 Para 2, "…capable of collecting RF signals between 40MHz and 6GHz and analyze 4G/5G/Wi-Fi internet signals of interest," The frequency range specified is wider than the frequency ranges indicated. Please indicate if other technologies in which you wish to find the threats are required – cellular 2G, 3G, Bluetooth, 2W-Radio, IOT

Response
RF signals between 40 MHz and 6 GHz, as well as the ability to characterize internet signals-of-interest from IP-based devices such as Wi-Fi/4G (5G)

76. Question: What level of concurrent bandwidth processing is desired for the Prototype? 100 MHz? 500 MHz? 1 GHz? 3 GH? 6 GHz? This will affect both the cost and SWaP of the Prototype and follow-on systems.

Response
The concurrent bandwidth has not been specified. Vendors may propose any unique solution to address the problem.

77. Question: In addition to 4G/5G/WiFi signals mentioned, is there interest in the RFSD identification of other wireless technologies transmitting in same 40MHz-6GHz range?

Response
See response to question 75.

78. Question: Do you have specific data base to train RFDS models, (mentioned as "baseline") or do we need to generate our own RF signals for database creation?

Response
See response to question 24 and 25.

79. Question: In reference to Project Deliverable #2; A software tool that is capable of scraping the internet to detect threats to DoD interests abroad. Would the government extend any special authorities to conduct open source exploitation in order to validate the solution using live data? Would the government envision utilizing language and socio-cultural experts? If so, What are these cultures, languages and dialects?

Response
See response to question 1 and 21.

80. Question: Can you clarify the intent of Deliverable 2, the internet scraping software?
a. Is the intent that RF signals in the operating environment which constitute internet traffic be scraped?
b. Are there any anticipated privacy concerns related to this software?

Response
See response to question 1.

81. Question: What percentage of the work is expected to be performed at NSWC Crane?

Response
There is no stated percentage or expectation of a certain percentage of the work expected to be performed at NSWC Crane, and performance at NSWC Crane is dependent on proposed solutions.

82. Question: Is the tables of contents included towards the 20 page count limit?

Response
No, it does not count toward the 20 page limit.

83. Question: What type of moving emitters should be considered in the prototype design?

Response
The RF signal device must detect emitters between 40 MHz and 6 GHz.

See response to question 75.

84. Question: Assuming geolocation is required, will three (or more) prototypes be procured?

Response
Vendors may propose any unique solution to address the problem.

See response to question 12.

85. Question: For geolocation communications between stations during testing, what type of network should we assume? Should we plan to provide our own or will one be provided. If the latter, what interface, bandwidth and latency may be assumed?

Response

Vendors may propose any unique solution to address the problem.

86. Question: For the prototype, what level of multipath discrimination is required?

Response
Level of multipath discrimination has not been specified. However, vendors may propose any unique solution to address the problem.

87. Question: For the prototype, is emitter fingerprinting required or desired? Is there a standard?

Response
Emitter fingerprinting has not been specified. However, vendors may propose any unique solution to address the problem.

88. Question: For the prototype demonstration, will the system be generating the background spectrum environment, or will it be provided? If the latter, what format?

Response
See response to question 62.

89. Question: Please specify the requirements for microelectronics to be considered "trusted"?

Response
See response to question 45.

90. Question: Is the Prototype to focus on commercial signals or are military signals and signals with active measures to reduce the probability of intercept to also be considered?

Response
All signals from 40 MHz to 6 GHz, as well as Wi-Fi/4G (5G) are signals of interest.

91. Question: Does the software tool search for false narratives and propaganda from journalist, news websites, message boards, etc? How does this tool address security threats? Does it harden the RFSD from cyber attack?

Response
There is no requirement to monitor the internet.

See response to question 1.

92. Question: Is the government interested in partial solutions, e.g., systems which perform the RF monitoring and alerting without the internet searching?

Response
Vendors may propose any unique solution to address the problem.

93. Question: If a unique partial solution exists does the Government desire it to be proposed? For example, say an RF sensor in a particularly interesting area of the spectrum that is low-cost, small and easily

deployable is possible. Does the Government intend to award multiple contracts are recommend small solution be merged with a lead integrator?

Response
See response to question 92.

94. Question: In order to provide the amount of detail requested in the Price Response, can the 5 page limitation be removed? The RFS states that providing BOE's could expedite the review process. Are BOE's to be provided as an attachment? Assume no page limitation.

Response
The 5 page limitation is increase to 8 pages maximum. The BOEs can be provided as an attachment and would not count against the 8 page limit in the price response.

95. Question: Please confirm that the analysis and threat indication should be based on the signal characteristic and not on its content (voice, video, data).

Response
Exploiting the signal being collected has not been specified. Vendors may propose any unique solution to address the problem.

96. Question: What is the meaning of "other spectrum communication?"

Response
All signals from 40 MHz to 6 GHz, as well as Wi-Fi/4G (5G) are signals of interest.

97. Question: Sect 5 Phase 2 Para 3, "The selected performer(s) will need to produce a prototype…" Should we produce a second prototype?

Response
Vendors may propose any unique solution to address the problem.

98. Question: What are the threats expected to be detected? (UAV, drones, remote attack, in house attack, visitors, personnel, passer-by, etc)

Response
All the devices listed may constitute potential threats.

99. Question: What GFI/GFE is provided?

Response
No GFE has been specified.

100. Question: For Phase 1 efforts, will the government provide equipment/devices generating the RF reference signals/waveforms for testing at the contractor facility.

Response

The vendor is required to demonstrate RF detection of equipment/devices generating the RF reference signals/waveforms during testing.

101. **Question**: Will the government consider an extension to the current due date of 15 June to 29 June, as teleworking and social distancing is an ongoing concern with collaboration due to the pandemic, the extra time is requested to ensure a quality submission?

Response

No

102. **Question**: The specification seems to be for two independent capabilities. Spectrum awareness and Internet analysis. If the kit is to be deployed in remote regions for the purpose of spectrum awareness it is unlikely the units will have simultaneous access to high bandwidth internet connections. Is it acceptable to propose a solution to one of these problems and not the other?

Response

See response to question 92

103. **Question**: Pursuant to question 1, is it permissible to propose two systems each individually optimized for the respective capabilities? It seems contra-purpose to increase the SWAP for the spectrum awareness capability if for many applications when used the internet analysis cannot be used at the same time.

Response

See response to question 93

104. **Question**: On 23 April, the FCC released 1.2 GHz of unlicensed spectrum in the 6 GHz band, this is likely in the near future to lead to the development of multitudes of devices from 5.925 to 7.125 GHz. Limiting the capability to 6 GHz could render the system obsolete before it is fielded. Recommend the minimum upper frequency limit be increased to support known near term frequency use.

Response

Vendors may propose any unique solution to address the problem.

105. **Question**: With respect to Paragraph 6, Line 1, please clarify the desired capabilities relative to signal analysis. For example, will demodulation of all signals be expected? Also, is it a requirement for the system to be able to decrypt the demodulated signals or is the ability to export this data to tools that are not part of this contract adequate? If part of this contract, please clarify capability desired. If not please clarify the export formats required.

Response

Exploitation of signals has not been specified. Vendors may propose any unique solution to address the problem.

106. **Question**: With respect to Paragraph 6, Line 2, please provide more detail as to what capabilities are to be supported) in more detail. For example, what is the response time required / expected for actionable data? Will translation of languages be limited or expected for all languages? Will the classification of the data gathered be performed by a third party or will guidelines be issued?

Response

See response to question 12 and 21.

107. **Question**: In Paragraph 6, Line 3 is there a standard for data output that is expected to be met? What is the expected alerting mechanism for actionable intelligence?

Response

A data output has not been specified. Vendors may propose any unique solution to address the problem.

See response to question 31.

108. **Question**: The Project deliverables mention software tool for scraping the internet and a virtual database for data storage. However, the RFS doesn't elaborate on these other than mentioning and issue with supply chain. These two deliverables seem unrelated to the primary subject of the RFS.

a. Is there more to this side of the request?
b. Is there more detail on either of these two desired capabilities?

Response

See response to question 1 and 45.

109. **Question**: Cyber Electromagnetic Activities (CEMA) (including friendly interference, compatibility, and vulnerability and threat intrusion, jamming, and interference) are increasingly jeopardizing the survivability and security of DOD assets and infrastructure.

a. Does RFSD need to consider Cyber Electromagnetic Activities (CEMA) or Cyber Security with IoT?
b. Identify Cyber Attacks on Mesh Networks, IoT, and Cellular Systems?

Response

Vendors may propose any unique solution to address the problem.

110. **Question**: What mechanisms are desired to be employed to counter the emerging threats? Jamming, spoofing, DF / Geo-location, Proposed CM? (E.g. Weapons designation)

Response

See response to question 12 and 22.

111. **Question**: What level of autonomy is proposed?

a. Command and Control of Sensor System?
b. Warnings, Firing Solutions, Geo-locations, proposed counter measures?

- E.g. command and control systems, tactical radios, information technology, assured position navigation and timing (APNT), radars, and missile fire control systems.

Response

See response to question 9 and 17.

112. **Question**: UAVs are listed as a threat, Are we only a identifying them with RF sensors or are acoustic sensors also being used?

Response

Vendors may propose any unique solution to address the problem.

113. **Question**: Are there any other specific threats other than IED and UAV?

Response

See response to question 98

114. **Question**: What Threats and in which frequency bands are of greatest interests?

a. Commercial Telecommunications? Or Tactical Radios?
b. Is the concern, primarily for short range communications, under 5km?
    - (Both Urban and Rural?)
c. Is Satellite Communications a concern?
d. What are the frequency bands to be covered?
    - DC to daylight? 550 kHZ to 25 GHz?
e. What is the sensitivity?
f. What is the desired detection range as a function of frequency?

Response

All signals from 40 MHz to 6 GHz, as well as Wi-Fi/4G (5G) are signals of interest.

115. **Question**: Is the greatest concern for signals in the local proximity within 5 km? The RFSD is basically not as concerned with signal capture outside 5 km?

Response

Maximum range has not been specified. Vendors may propose any unique solution to address the problem.

116. **Question**: The reference proposed RF networks that are low range and high data through-put, will these be of greatest concern or concentration?

Examples:

- A few IoT networks:
  LoRaWAN, SigFox, Telsensa, Nwave, Weightless, NB-Fi, WiMAX, ZigBee, BLE, Z-Wave, Thread, Wi-Fi (802.11), 3G, 4G, 5G, LTE
- A few commonly used modulations:
  AM, FM, PM, OOK, FSK, PSK, TDMA, CDMA, FDMA, SDMA, DSSS, CSS, FHSS, THSS

Response

See response to question 114

1. What is the platform for the required solution (Naval, Fixed-Location, Airborne) and in what environment (Urban, Suburban, Rural)? Is there a preferred means for alert delivery and what metadata should be included? Who is the intended User/Customer?
(Q. 31, 34, 65, 71)

The solutions for Phase III will be evaluated at a fixed facility
The system should be configured for urban environments.
An alert delivery has not been specified.
USCENTCOM is the intended customer.

2. Is the desired system SWaP constrained? Is there an operational time and life requirement?
(Q. 7, 8, 35, 56, 61)

The solution must conform to transport by a military helicopter.

3. Is this scraping tool mainly looking at internet traffic across the RF being monitored? Is the device expected to correlate a scraped event from the internet to a particular RF event being sensed? Does scraping the internet only include off the air (4G/5G/Wi-Fi) and not wired? Does the scope of the software tool include monitoring IP packets that are transmitted or received by DoD devices?
(Q. 1, 2, 3, 4, 5, 6, 13, 45, 63, 79, 80, 108)

Any internet tool would primarily be looking at internet traffic as it pertains to a communications path.
The capability of the internet/Wi-Fi/IP traffic monitoring is dependent on the vendor solution.
IP traffic would be limited to 4G/5G/Wi-fi-type signals.
DoD devices have not been specified as target platforms.

4. Should the software tool learn the network health and baseline *a posteriori*, through interaction with the environment? Or, should the system incorporate some pre-defined baseline, perhaps as a function of locale or region? For the prototype demonstration, will the system be generating the background spectrum environment, or will it be provided?
(Q. 17, 62, 88)

The vendor is responsible for proposing a solution to provide baseline assessments.

5. In addition to 4G/5G/WiFi signals mentioned, is there interest in the RFSD identification of other wireless technologies transmitting in same 40MHz-6GHz range? Does RFSD need to consider Cyber Electromagnetic Activities (CEMA) or Cyber Security with IoT? What are the threats expected to be detected (UAV, drones, remote attack, in house attack, visitors, personnel, passer-by, etc)?
(Q. 74, 75, 77, 83, 98, 111, 113)

RF signals between 40 MHz and 6 GHz, as well as the ability to characterize internet signals-of-interest from IP-based devices such as Wi-Fi/4G (5G).
All the devices listed may constitute potential threats.