Office of the Under Secretary of Defense for Research and Engineering
FutureG Office
24.3 Small Business Innovation Research (SBIR)
Proposal Submission Instructions

May 16, 2024: Topics issued for pre-release
May 28, 2024: OUSD(R&E) begins accepting proposals via DSIP
June 25, 2024: DSIP Topic Q&A closes to new questions at 12:00 p.m. ET
July 9, 2024: Deadline for receipt of proposals no later than 12:00 p.m. ET

INTRODUCTION

The Office of the Undersecretary of Defense, Research and Engineering's (OUSD(R&E's)) FutureG Office (FutureG) aims to ensure DoD can securely operate through or make use of existing commercial 5G networks in any environment by delivering clear and actionable security assurances and providing enhancements and augmentation to a combination of the end user device and the existing communications infrastructure.

Proposers responding to a topic in this Broad Agency Announcement (BAA) must follow all general instructions provided in the Department of Defense (DoD) SBIR Program BAA. OUSD(R&E) FutureG requirements in addition to or deviating from the DoD Program BAA are provided in the instructions below.

Proposers are encouraged to thoroughly review the DoD Program BAA and register for the DSIP Listserv to remain apprised of important programmatic and contractual changes.

- The DoD Program BAA is located at: https://www.defensesbirsttr.mil/SBIR-STTR/Opportunities/ and https://www.defensesbirsttr.mil/SBIR-STTR/announcements. Be sure to select the tab for the appropriate BAA cycle.
- Register for the DSIP Listserv at: https://www.dodsbirsttr.mil/submissions/login.

Specific questions pertaining to the administration of the OUSD(R&E) FutureG SBIR Program and these proposal preparation instructions should be directed to: Brian D. Saunders at Brian.D.Saunders2.ctr@mail.mil.

This release contains an open topic. As outlined in section 7 of the SBIR and STTR Extension Act of 2022, innovation open topic activities—

(A) Increase the transition of commercial technology to the Department of Defense;
(B) Expand the small business nontraditional industrial base;
(C) Increase commercialization derived from investments of the Department of Defense; and
(D) Expand the ability for qualifying small business concerns to propose technology solutions to meet the needs of the Department of Defense.

Unlike conventional topics, which specify the desired technical objective and output, open topics can use generalized mission requirements or specific technology areas to adapt commercial products or solutions to close capability gaps, improve performance, or provide technological advancements in existing capabilities.

A small business concern may only submit one (1) proposal to each open topic. If more than one proposal from a small business concern is received for a single open topic, only the most recent proposal to be certified and submitted prior to the submission deadline will receive an evaluation. All prior proposals submitted by the small business concern for the same open topic will be marked as nonresponsive and will not receive an evaluation.

PHASE I PROPOSAL GUIDELINES

The Defense SBIR/STTR Innovation Portal (DSIP) is the official portal for DoD SBIR/STTR proposal submission. Proposers are required to submit proposals via DSIP; proposals submitted by any other means will be disregarded. Detailed instructions regarding registration and proposal submission via DSIP are provided in the DoD SBIR Program BAA.

Technical Volume (Volume 2)

The technical volume is not to exceed twelve (12) pages of written text. Eight (8) additional pages of content such as graphics and charts that describe aspects of the solution and the company are allowed but not required. Technical volume beyond the twenty (20) pages will not be considered for evaluation purposes.

Additional formatting and content requirements are provided in the DoD Program BAA.

Cost Volume (Volume 3)

The Phase I Base amount must not exceed $295,000. Costs must be clearly identified on the Proposal Cover Sheet (Volume 1) and in Volume 3.

Please review the updated Percentage of Work (POW) calculation details included in the DoD Program BAA. OUSD(R&E) FutureG will occasionally accept deviations from the POW requirements with written approval from the Funding Agreement officer.

Company Commercialization Report (CCR) (Volume 4)

Completion of the CCR as Volume 4 of the proposal submission in DSIP is required. Please refer to the DoD SBIR Program BAA for full details on this requirement. Information contained in the CCR will be considered by OUSD(R&E) FutureG during proposal evaluations.

Supporting Documents (Volume 5)

All proposing small business concerns are REQUIRED to submit the following documents to Volume 5:

1. Contractor Certification Regarding Provision of Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
2. Disclosures of Foreign Affiliations or Relationships to Foreign Countries

Please refer to the DoD Program BAA for more information.

PHASE II PROPOSAL GUIDELINES

Phase II proposals may only be submitted by Phase I awardees. Phase I awardees will receive a separate notification with detailed instructions and timelines for Phase II proposal submission.

DISCRETIONARY TECHNICAL AND BUSINESS ASSISTANCE (TABA)

OUSD(R&E) FutureG will not provide technical and business assistance for this open topic.

EVALUATION AND SELECTION

All proposals will be evaluated in accordance with the evaluation criteria listed in the DoD SBIR Program BAA.

Proposing firms will be notified of selection or non-selection status for a Phase I award within 90 days of the closing date of the BAA. All notifications will be made to the corporate official and principal investigator identified on the proposal coversheet.

Refer to the DoD SBIR Program BAA for procedures to protest the Announcement.
As further prescribed in FAR 33.106(b), FAR 52.233-3, protests after award should be submitted to:

Defense SBIR/STTR Program Office
osd.ncr.ousd-r-e.mbx.SBIR-STTR-Protest@mail.mil

END

OSD (FutureG) 24.4 SBIR Topic Index
Release 2

OSD243-P002	Development of novel 5G Open RAN (Radio Access Networks) xApp and rApp Applications

OSD244-P002 TITLE: Development of novel 5G Open RAN (Radio Access Networks) xApp and rApp Applications Open Topic

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): FutureG; Sustainment & Logistics

OBJECTIVE: The Department of Defense (DoD) is seeking the development and demonstration of xApps and/or rApps focused on security and security related network measurement. DoD anticipates increasing reliance on 5G and FutureG OpenRAN networks, and needs tools and techniques that will enhance the security and resilience of these networks. As 5G networks facilitate a wider array of services and accommodate an ever-increasing number of connected devices, they become prime targets for sophisticated cyber-attacks. These networks provide an open communication surface through which devices and base stations can be exposed to hostile cellular activities, interference, and both known and unknown vulnerabilities that exist within the protocol standards. There is an emerging recognition of opportunities presented by the xApp and rApp framework to increase the trustworthiness and reliability of OpenRAN networks from malicious activities. By providing detailed insights into network performance and security metrics, these applications can enable a more nuanced understanding of the network's security posture, and can help mitigate a wide range of potential attacks. The primary use case is in support of DoD network operators, owners, and users who depend upon reliable and trustworthy network communications in support of various DoD missions.

DESCRIPTION: FutureG within the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E) seeks innovative security-focused xApp and rApp application solutions. xApps and rApps represent significant differentiators in the evolution of 5G (and beyond) wireless networking, and are poised to drive rapid innovations beyond what has been achievable in legacy wireless network architectures. These applications, integral to the OpenRAN architecture, embody a transformative approach to network management and efficiency, underpinned by the principles of openness, intelligence, and programmability. The integration of xApps and rApps within the OpenRAN framework represents an opportunity for a significant step forward in securing 5G networks. By leveraging these applications, network operators can enhance their ability to detect, analyze, and mitigate a wide range of security threats in real-time.

OpenRAN and the RAN Intelligent Controller (RIC) enable new innovations in cellular network operations, and the development and deployment of xApps and rApps will be a critical driver for Open RAN adoption and deployment. Currently existing xApps and rApps have focused on topics such as energy efficiency, spectrum management, and improved resource management, however to date there are fewer xApps and rApps that provide enhanced security features or allow for security and security measurement. As the Open RAN landscape continues to evolve, FutureG is looking for the development and deployment of security-focused xApps and rApps that will be paramount in providing the necessary agility and resilience necessary to maintain the trustworthiness of 5G (and beyond) wireless network ecosystems. Proposed solutions should focus on expanding the capabilities of xApps and rApps to address emerging threats and enhancing the scalability and efficiency of these applications to support the growing demands of cellular networks. The identification of the security threat/vulnerability, as well as its mitigation, is in scope. An example would be the identification and pinpointing of interference or identification and pinpointing of rogue base stations, based on neighbors reported by UEs and comparing with lists of legitimate neighbors. Solutions that leverage artificial intelligence (AI) and machine learning (ML) for predictive security are encouraged, but the use of AI and ML is not required. These aspect areas are merely guidelines for the proposer, and DoD will entertain additional ideas that provide potential for increased security and resiliency. Warfighter communication scenarios are sometimes different than commercial scenarios, and this aspect should also be considered when proposing xApps and rApps in response to this topic as there may be relevant dual-use cases for the applications to be deployed in commercial and DoD networks.

PHASE I: In Phase 1, the proposer should present a design for at least one high quality xApp or rApp idea, however they may propose more than one provided that they are of equal quality and anticipated impact, or the multiple applications provide interlinked dependencies.

Solutions proposed in response to this topic will be assessed by focusing on several evaluation areas and metrics such as:

- Overall impact of proposed solution
- False positive/false negative rate
- Complexity of operational problem to be addressed
- Mean time to detect, contain, resolve, and recover
- Vulnerability identification rate
- Time to resolve identified vulnerability
- Adaptability/extensibility to address evolving operational landscape
- Policy/regulatory compliance
- Adherence to established standards and protocols

It is expected that the general evaluation areas and metrics descriFutureG within the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E) seeks innovative security-focused xApp and rApp application solutions. xApps and rApps represent significant differentiators in the evolution of 5G (and beyond) wireless networking, and are poised to drive rapid innovations beyond what has been achievable in legacy wireless network architectures. These applications, integral to the OpenRAN architecture, embody a transformative approach to network management and efficiency, underpinned by the principles of openness, intelligence, and programmability. The integration of xApps and rApps within the OpenRAN framework represents an opportunity for a significant step forward in securing 5G networks. By leveraging these applications, network operators can enhance their ability to detect, analyze, and mitigate a wide range of security threats in real-time.

OpenRAN and the RAN Intelligent Controller (RIC) enable new innovations in cellular network operations, and the development and deployment of xApps and rApps will be a critical driver for Open RAN adoption and deployment. Currently existing xApps and rApps have focused on topics such as energy efficiency, spectrum management, and improved resource management, however to date there are fewer xApps and rApps that provide enhanced security features or allow for security and security measurement. As the Open RAN landscape continues to evolve, FutureG is looking for the development and deployment of security-focused xApps and rApps that will be paramount in providing the necessary agility and resilience necessary to maintain the trustworthiness of 5G (and beyond) wireless network ecosystems. Proposed solutions should focus on expanding the capabilities of xApps and rApps to address emerging threats and enhancing the scalability and efficiency of these applications to support the growing demands of cellular networks. The identification of the security threat/vulnerability, as well as its mitigation, is in scope. An example would be the identification and pinpointing of interference or identification and pinpointing of rogue base stations, based on neighbors reported by UEs and comparing with lists of legitimate neighbors. Solutions that leverage artificial intelligence (AI) and machine learning (ML) for predictive security are encouraged, but the use of AI and ML is not required. These aspect areas are merely guidelines for the proposer, and DoD will entertain additional ideas that provide potential for increased security and resiliency. Warfighter communication scenarios are sometimes different than commercial scenarios, and this aspect should also be considered when proposing xApps and rApps in response to this topic as there may be relevant dual-use cases for the applications to be deployed in commercial and DoD networks.

In Phase 1, the proposer should present a design for at least one high quality xApp or rApp idea, however they may propose more than one provided that they are of equal quality and anticipated impact, or the multiple applications provide interlinked dependencies.

Solutions proposed in response to this topic will be assessed by focusing on several evaluation areas and metrics such as:

- Overall impact of proposed solution
- False positive/false negative rate
- Complexity of operational problem to be addressed
- Mean time to detect, contain, resolve, and recover
- Vulnerability identification rate
- Time to resolve identified vulnerability
- Adaptability/extensibility to address evolving operational landscape
- Policy/regulatory compliance
- Adherence to established standards and protocols

It is expected that the general evaluation areas and metrics described here will be expanded into more granular metrics during the development of the solution.

Phase Description and Timeline:

PHASE I – SIX MONTHS: Develop initial application concept and design document for development and deployment of the applications. Phase I will be a 6-month Period of Performance (PoP). During this period there will be a kickoff, Technical Interchange Meeting (TIM), and a Preliminary Design Review (PDR). Prior to the end of Phase I, the performer will develop and present a proposed, detailed plan related to how they expect to address Phase II prototype production, test, and evaluation efforts. There will be a downselection prior to the start of Phase II. Simply meeting stated goals and milestones during Phase I may not be sufficient to to be invited to advance to Phase II, and FutureG reserves the right to evaluate Phase II candidate solutions along other criteria such as likelihood of transition, technical complexity, and available resources.

Deliverables: Kick off and TIM slides, monthly status reports (MSRs), Preliminary Design Document, Phase II Plan, Final Phase I Report.

The proposer will include a plan for implementing the FutureG Cybersecurity Model. The model will be provided following Phase I selection.

PHASE II: PHASE II – TWELVE MONTHS: During Phase II, the Phase I selected performer(s) will begin the prototype production and test and evaluation process. Phase II will be a 12-month PoP with a kick off and TIM at month 1, Critical Design Review at month six (6), prototype demonstration at month nine (9) and a final design and security review/red teaming at month 11.

Prototype demonstration will be conducted at a DoD selected location, during which the solution's capabilities must be successfully demonstrated. For budget and planning purposes, proposals should assume the test facility will be a DoD provided environment. Test facilities may vary and will be determined early in Phase II. A partial solution may be determined to be successful if the DoD determined it to be effective in a limited role. A final technical report of the prototype capabilities as demonstrated at the Final Demonstration will also be required. Extended user evaluations or additional prototypes may be pursued to determine utility.

Deliverables: Kick off and TIM slides, MSRs, Critical Design Document, Prototype Demonstration Slides and Documentation, Final Design Document, Final Technical Report.

The proposer will apply the FutureG Cybersecurity Model and complete/document necessary actions. The model will be provided following Phase I selection.

PHASE III DUAL USE APPLICATIONS: Phase IIIs will be determined on an as-needed basis to address additional needed capability development not covered in Phase II or to cover activities related to transition to operational use.

REFERENCES:

1. U.S. Patent application – US18/012,129 Network aware compute resource management use case for o-ran non-rt ric

KEYWORDS: 5G, Open RAN, xApp, rApp, O-RAN, RAN Intelligent Controller (RIC), Network.

TPOC-1: Daniel Massey
Email: Daniel.F.Massey3.civ@mail.mil