DEPARTMENT OF THE NAVY (DON)
Small Business Innovation Research (SBIR)
DoW 2026 SBIR BAA Release 3
Phase I Proposal Submission Instructions

IMPORTANT

- **The following instructions apply to topics:**
  - **DON26BZ03-NV054 through DON26BZ03-NV065**

- Submitting small business concerns (SBCs) are encouraged to thoroughly review the DoW SBIR/STTR Program Broad Agency Announcement (BAA) and register for the DSIP Listserv to remain apprised of important programmatic changes.
  - The DoW Program BAA is located at: https://www.dodsbirsttr.mil/submissions/login. Select the tab for the appropriate BAA cycle.
  - Register for the DSIP Listserv at: https://www.dodsbirsttr.mil/submissions/login.

- The information provided in the DON Proposal Submission Instructions takes precedence over the DoW Instructions posted for this BAA.

- **DON Phase I Technical Volume (Volume 2) page limit is not to exceed 10 pages.**

- Proposing SBCs that are more than 50% owned by multiple venture capital operating companies (VCOC), hedge funds (HF), private equity firms (PEF) or any combination of these are eligible to submit proposals in response to DON topics advertised in this BAA. Information on Majority Ownership in Part and certification requirements at time of submission for these proposing SBCs are detailed in the section titled ADDITIONAL SUBMISSION CONSIDERATIONS.

- Phase I Technical Volume (Volume 2) and Supporting Documents (Volume 5) templates, specific to DON topics, are available at https://www.navysbir.com/links_forms.htm.

- The DON may consider the following FAR and Non-FAR contract strategies when issuing Phase I awards: Firm Fixed Price (FFP), Basic Ordering Agreement (BOA), or Prototype Other Transaction (OT). The DON may consider the following FAR and Non-FAR contracting strategies when issuing Phase II awards: Cost Plus Fixed Fee (CPFF), FFP, BOA, or Prototype OT.

- This BAA is issued under regulations set forth in Federal Acquisition Regulation (FAR) 35.016 and awards will be made under "other competitive procedures". The policies and procedures of FAR Subpart 15.3 shall not apply to this BAA, except as specifically referenced in it. All procedures are at the sole discretion of the Government as set forth in this BAA. Submission of a proposal in response to this BAA constitutes the express acknowledgement to that effect by the proposing SBC.

INTRODUCTION

The DON SBIR/STTR Programs are mission-oriented programs that integrate the needs and requirements of the DON's Fleet through research and development (R&D) topics that have dual-use potential, but primarily address the needs of the DON. More information on the programs can be found on the DON SBIR/STTR website at www.navysbir.com. Additional information on DON's mission can be found on the DON website at www.navy.mil.

For questions regarding this BAA, use the information in Table 1 to determine who to contact for what types of questions.

TABLE 1: POINTS OF CONTACT FOR QUESTIONS REGARDING THIS BAA

Type of Question	When	Contact Information
Program and administrative	Always	Navy SBIR/STTR Program Management Office usn.pentagon.cnr-arlington-va.mbx.navy-sbir-sttr@us.navy.mil or appropriate Program Manager listed in Table 2 (below)
Topic-specific technical questions	BAA Pre-release	Technical Point of Contact (TPOC) listed in each topic on the DoW SBIR/STTR Innovation Portal (DSIP). Refer to the Proposal Submission section of the DoW SBIR/STTR Program BAA for details.
	BAA Open	DoW SBIR/STTR Topic Q&A platform (https://www.dodsbirsttr.mil/submissions) Refer to the Proposal Submission section of the DoW SBIR/STTR Program BAA for details.
Electronic submission to the DoW SBIR/STTR Innovation Portal (DSIP)	Always	DSIP Support via email at dodsbirsupport@reisystems.com
Navy-specific BAA instructions and forms	Always	DON SBIR/STTR Program Management Office usn.pentagon.cnr-arlington-va.mbx.navy-sbir-sttr@us.navy.mil

TABLE 2: DON SYSTEMS COMMANDS (SYSCOM) SBIR PROGRAM MANAGERS

Topic Numbers	Point of Contact	SYSCOM	Email
DON26BZ03-NV054	Ms. Tatiana Sears	Marine Corps Systems Command (MCSC)	smb_mcsc_sbir_admins@usmc.mil
DON26BZ03-NV055 to DON26BZ03-NV065	Mr. Jason Schroepfer	Naval Sea Systems Command (NAVSEA)	NSSC_SBIR.fct@navy.mil

PHASE I SUBMISSION INSTRUCTIONS

The following section details requirements for submitting a compliant Phase I proposal to the DoW SBIR/STTR Programs.

(NOTE: Proposing SBCs are advised that support contract personnel will be used to carry out administrative functions and may have access to proposals, contract award documents, contract deliverables, and reports. All support contract personnel are bound by appropriate non-disclosure agreements.)

DoW SBIR/STTR Innovation Portal (DSIP). Proposing SBCs are required to submit proposals via the DoW SBIR/STTR Innovation Portal (DSIP); and follow proposal submission instructions in the DoW SBIR/STTR Program BAA on the DSIP at https://www.dodsbirsttr.mil/submissions. Proposals submitted by any other means will be disregarded. Proposing SBCs submitting through DSIP for the first time will be asked to register. It is recommended that SBCs register as soon as possible upon identification of a proposal opportunity to avoid delays in the proposal submission process. Proposals that are not successfully certified electronically in DSIP by the Corporate Official prior to BAA Close will NOT be considered submitted and will not be evaluated by DON. Proposals that are encrypted, password protected, or otherwise locked in any portion of the submission will be REJECTED unless specifically directed within the text of the topic to which you are submitting. Please refer to the DoW SBIR/STTR Program BAA for further information.

Proposal Volumes. The following seven volumes are required.

- **Proposal Cover Sheet (Volume 1).** As specified in DoW SBIR/STTR Program BAA.

- **Technical Proposal (Volume 2)**
  - Technical Proposal (Volume 2) must meet the following requirements or the proposal will be REJECTED:
    - Not to exceed ten (10) pages, regardless of page content
    - Single column format, single-spaced typed lines
    - Standard 8 ½" x 11" paper
    - Page margins one inch on all sides. A header and footer may be included in the one-inch margin.
    - No font size smaller than 10-point
    - Include, within the ten-page limit of Volume 2, an Option that furthers the effort in preparation for Phase II and will bridge the funding gap between the end of Phase I and the start of Phase II. Tasks for both the Phase I Base and the Phase I Option must be clearly identified. Phase I Options are exercised upon selection for Phase II.
    - Work proposed for the Phase I Base must be exactly six (6) months.
    - Work proposed for the Phase I Option must be exactly six (6) months.

  - Additional information:
    - A Phase I proposal template specific to DON to meet Phase I requirements is available at https://navysbir.com/links_forms.htm
    - A font size smaller than 10-point is allowable for headers, footers, imbedded tables, figures, images, or graphics that include text. However, proposing SBCs are cautioned that if the text is too small to be legible it will not be evaluated.

- **Cost Volume (Volume 3).**
  - Cost Volume (Volume 3) must meet the following requirements or the proposal will be REJECTED:
    - The Phase I Base amount must not exceed $200,000.
    - Phase I Option amount must not exceed $115,000.
    - Costs for the Base and Option must be separated and clearly identified in Volume 3.
    - For Phase I, a minimum of two-thirds of the work is performed by the proposing SBC. The two-thirds percentage of work requirement must be met in the Base costs as well as in the Option costs. DON will not accept deviations from the minimum percentage of work requirements for Phase I. The percentage of work is measured by both direct and indirect costs. To calculate the minimum percentage of work for the proposing SBC the sum of all direct and indirect costs attributable to the proposing SBC represent the numerator and the total cost of the proposal (i.e., Total Cost before Profit Rate is applied) is the denominator. The subcontractor percentage is calculated by taking the sum of all costs attributable to the subcontractor (Total Subcontractor Costs (TSC)) as the numerator and the total cost of the proposal (i.e., Total Cost before Profit Rate is applied) as the denominator.
      - Proposing SBC Costs (included in numerator for calculation of the SBC):
        - Total Direct Labor (TDL)
        - Total Direct Material Costs (TDM)
        - Total Direct Supplies Costs (TDS)
        - Total Direct Equipment Costs (TDE)
        - Total Direct Travel Costs (TDT)
        - Total Other Direct Costs (TODC)
        - General & Administrative Cost (G&A)

        NOTE: G&A, if proposed, will only be attributed to the proposing SBC.
      - Subcontractor Costs (numerator for subcontractor calculation):
        - Total Subcontractor Costs (TSC)
      - Total Cost (i.e., Total Cost before Profit Rate is applied, denominator for either calculation)
    - **Cost Sharing: Cost sharing is not accepted on DON Phase I proposals. A value above or below $0.00 entered in the Cost Sharing field will not be considered in the Phase I contract award.**

  - Additional information:
    - Provide sufficient detail for subcontractor, material, and travel costs. Subcontractor costs must be detailed to the same level as the prime contractor. Material costs must include a listing of items and cost per item. Travel costs must include the purpose of the trip, number of trips, location, length of trip, and number of personnel.
    - Inclusion of cost estimates for travel to the sponsoring SYSCOM's facility for one day of meetings is recommended for all proposals.
    - The "Additional Cost Information" of Supporting Documents (Volume 5) may be used to provide supporting cost details for Volume 3. When a proposal is selected for award, be prepared to submit further documentation to the SYSCOM Contracting Officer to substantiate costs (e.g., an explanation of cost estimates for equipment, materials, and consultants or subcontractors).

- **Company Commercialization Report (Volume 4)**. DoW collects and uses Volume 4 and DSIP requires Volume 4 for proposal submission. Please refer to the Proposal Preparation Instructions and Requirements section of the DoW SBIR/STTR Program BAA for details to ensure compliance with DSIP Volume 4 requirements.

- **Supporting Documents (Volume 5).** Volume 5 is for the submission of administrative material that DON may or will require to process a proposal, if selected, for contract award.

  - Proposing SBCs must review and submit the following items, as applicable:
    - **Majority Ownership in Part.** Proposing SBCs that are more than 50% owned by multiple venture capital operating companies (VCOC), hedge funds (HF), private equity firms (PEF), or any combination of these as set forth in 13 C.F.R. § 121.702, are eligible to submit proposals in response to DON topics advertised within this BAA. Complete the certification as detailed under ADDITIONAL SUBMISSION CONSIDERATIONS.

  - Additional information:
    - Proposing SBCs may include the following administrative materials in Supporting Documents (Volume 5); a template is available at https://navysbir.com/links_forms.htm to provide guidance on optional material the proposing SBC may want to include in Volume 5:
      - Additional Cost Information to support the Cost Volume (Volume 3)
      - SBIR/STTR Funding Agreement Certification
      - Data Rights Assertion
      - Disclosure of Information (DFARS 252.204-7000)
      - Prior, Current, or Pending Support of Similar Proposals or Awards
      - Foreign Citizens
    - Details of Request for Discretionary Technical and Business Assistance (TABA), if proposed, is to be included under the Additional Cost Information section if using the DON Supporting Documents template.
    - Do not include documents or information to substantiate the Technical Volume (Volume 2) in Volume 5 (e.g., resumes, test data, technical reports, or publications). Such documents or information will not be considered.
    - A font size smaller than 10-point is allowable for documents in Volume 5; however, proposing SBCs are cautioned that the text may be unreadable.

  Fraud, Waste and Abuse Training (Volume 6). DoW requires Volume 6 for submission. Please refer to the Proposal Preparation Instructions and Requirements section of the DoW SBIR/STTR Program BAA for details.

- **Disclosures of Foreign Affiliations or Relationships to Foreign Countries (Volume 7)**. In accordance with Section 4 of the SBIR and STTR Extension Act of 2022 and the SBA SBIR/STTR Policy Directive, the DoW will review all proposals submitted in response to this BAA to assess security risks presented by SBCs seeking a Federally funded award. SBCs must complete the Disclosures of Foreign Affiliations or Relationships to Foreign Countries webform in Volume 7 of the DSIP proposal submission. Please refer to the Proposal Preparation Instructions and Requirements section of the DoW SBIR/STTR Program BAA for details.

PHASE I EVALUATION AND SELECTION

The following section details how the DON SBIR/STTR Programs will evaluate Phase I proposals.

Proposals meeting DSIP submission requirements will be forwarded to the DON SBIR/STTR Programs. Prior to evaluation, all proposals will undergo a compliance review to verify compliance with DoW and DON SBIR/STTR proposal eligibility requirements. Proposals not meeting submission requirements will be REJECTED and not evaluated.

- **Proposal Cover Sheet (Volume 1).** The Proposal Cover Sheet (Volume 1) will undergo a compliance review to verify the proposing SBC has met eligibility requirements and followed the instructions for the Proposal Cover Sheet as specified in the DoW SBIR/STTR Program BAA.

- **Technical Volume (Volume 2).** The DON will evaluate and select Phase I proposals using the evaluation criteria specified in the Method of Selection and Evaluation Criteria section of the DoW SBIR/STTR Program BAA, with technical merit being most important, followed by qualifications of key personnel and commercialization potential of equal importance. The information considered for this decision will come from Volume 2. This is not a FAR Part 15 evaluation and proposals will not be compared to one another. Cost is not an evaluation criterion and will not be considered during the evaluation process; the DON will only do a compliance review of Volume 3. Due to limited funding, the DON reserves the right to limit the number of awards under any topic.

  The Technical Volume (Volume 2) will undergo a compliance review (prior to evaluation) to verify the proposing SBC has met the following requirements or the proposal will be REJECTED:
  - Not to exceed ten (10) pages, regardless of page content
  - Single column format, single-spaced typed lines
  - Standard 8 ½" x 11" paper
  - Page margins one inch on all sides. A header and footer may be included in the one-inch margin.
  - No font size smaller than 10-point, except as permitted in the instructions above.
  - Include, within the 10-page limit of Volume 2, an Option that furthers the effort in preparation for Phase II and will bridge the funding gap between the end of Phase I and the start of Phase II. Tasks for both the Phase I Base and the Phase I Option must be clearly identified.
  - Work proposed for the Phase I Base must be exactly six (6) months.
  - Work proposed for the Phase I Option must be exactly six (6) months.

- **Cost Volume (Volume 3).** The Cost Volume (Volume 3) will not be considered in the selection process and will only undergo a compliance review to verify the proposing SBC has met the following requirements or the proposal will be REJECTED:
  - Must not exceed values for the Base ($200,000) and Option ($115,000).
  - Must meet minimum percentage of work; a minimum of two-thirds of the work is performed by the proposing SBC. The two-thirds percentage of work requirement must be met in the Base costs as well as in the Option costs. DON will not accept deviations from the minimum percentage of work requirements for Phase I.
  - **Cost Sharing: Cost sharing is not accepted on DON Phase I proposals. A value above or below $0.00 entered in the Cost Sharing field will not be considered in the Phase I contract award.**

- **Company Commercialization Report (CCR) (Volume 4).** The CCR (Volume 4) will not be evaluated by the DON nor will it be considered in the award decision. However, all proposing SBCs must refer to the DoW SBIR/STTR Program BAA to ensure compliance with DSIP Volume 4 requirements.

- **Supporting Documents (Volume 5).** Supporting Documents (Volume 5) will not be considered in the selection process and will only undergo a compliance review to ensure the proposing SBC has included items in accordance with the PHASE I SUBMISSION INSTRUCTIONS section above.

- **Fraud, Waste, and Abuse Training Certificate (Volume 6).** Not evaluated.

- **Disclosures of Foreign Affiliations or Relationships to Foreign Countries (Volume 7)**. Disclosures of Foreign Affiliations or Relationships to Foreign Countries (Volume 7) will be assessed as part of the Due Diligence Program to Assess Security Risks. Refer to the DoW SBIR/STTR Program BAA to ensure compliance with Volume 7 requirements.

ADDITIONAL SUBMISSION CONSIDERATIONS

This section details additional items for proposing SBCs to consider during proposal preparation and submission process.

Due Diligence Program to Assess Security Risks. The SBIR and STTR Extension Act of 2022 (Pub. L. 117-183) requires the Department of War, in coordination with the Small Business Administration, to establish and implement a due diligence program to assess security risks presented by SBCs seeking a Federally-funded award. Please review the Certifications and Registrations section of the DoW SBIR/STTR Program BAA for details on how DoW will assess security risks presented by SBCs. The Due Diligence Program to Assess Security Risks will be implemented for all Phases.

Discretionary Technical and Business Assistance (TABA). The Small Business Innovation and Economic Security Act Section 7 mandates agencies offer TABA. The purpose of TABA is to assist awardees in making better technical decisions on SBIR/STTR projects; solving technical problems that arise during SBIR/STTR projects; minimizing technical risks associated with SBIR/STTR projects; commercializing the SBIR/STTR product or process, including intellectual property protections and cybersecurity assistance; and screening for potential foreign involvement in technology development or commercialization activities. TABA services can be provided through vendor(s) selected by the SBC or the SBC may propose use of TABA funding to hire new staff, augment staff, or direct staff to conduct or participate in training activities consistent with the purpose of TABA as detailed above. The Phase I TABA amount, if proposed, cannot include any profit/fee by the proposing SBC and must be inclusive of all applicable indirect costs. TABA cannot be used in the calculation of general and administrative expenses (G&A) for the SBIR proposing SBC. An SBC receiving TABA will be required to submit a report detailing the results and benefits of the service received. This TABA report will be due at the time of submission of the final report.

Request for TABA funding will be reviewed by the DON SBIR/STTR Program Management Office.

If proposing a TABA Provider, the following MUST be included in the request or be subject to denial.
- Provider(s)
- Provider(s) point of contact, email address, and phone number
- An explanation of the provider's unique qualifications to provide the TABA service
- Tasks that will be performed by the provider (to include the purpose and objective of the assistance)
- Total provider(s) cost, number of hours, and labor rates (average/blended rate is acceptable)

If proposing TABA funding to hire new staff, augment staff, or direct staff to conduct or participate in training activities consistent with the purpose of TABA, the following MUST be included or be subject to denial.
- Name(s), position(s), business need to be filled, and/or training to be provided
- Number of employees to be hired, augmented, or directed to participate in training activities
- Qualifications of employees hired or augmented, or detailed need for training
- Tasks that will be performed (to include the purpose and objective of the assistance)

- Total staff/training cost, number of hours, and labor rates (average/blended rate is acceptable)

TABA requests must be included in the proposal as follows:

- Phase I:
  - Online DoW Cost Volume (Volume 3) – the value of the TABA request.
  - Supporting Documents (Volume 5) – a detailed request for TABA (as specified above) specifically identified as "TABA" in the section titled Additional Cost Information when using the DON Supporting Documents template.
- Phase II:
  - DON Phase II Cost Volume (provided by the DON SYSCOM) - the value of the TABA request.
  - Supporting Documents (Volume 5) – a detailed request for TABA (as specified above) specifically identified as "TABA" in the section titled Additional Cost Information when using the DON Supporting Documents template.

Proposed values for TABA must NOT exceed:

- Phase I: A total of $6,500, in addition to the Phase I award amount.
- Phase II: A total of $25,000 per award, not to exceed $50,000 per Phase II project, included in the Phase II award amount.

Disclosure of Information (DFARS 252.204-7000). In order to eliminate the requirements for prior approval of public disclosure of information (in accordance with DFARS 252.204-7000) under this award, the proposing SBC shall identify and describe all fundamental research to be performed under its proposal, including subcontracted work, with sufficient specificity to demonstrate that the work qualifies as fundamental research. Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons (defined by National Security Decision Directive 189). An SBC whose proposed work will include fundamental research and requests to eliminate the requirement for prior approval of public disclosure of information must complete the DON Fundamental Research Disclosure and upload as a separate PDF file to the Supporting Documents (Volume 5) in DSIP as part of their proposal submission. The DON Fundamental Research Disclosure is available on https://navysbir.com/links_forms.htm and includes instructions on how to complete and upload the completed Disclosure. Simply identifying fundamental research in the Disclosure does **NOT** constitute acceptance of the exclusion. All exclusions will be reviewed and, if approved by the Government Contracting Officer, noted in the contract.

Majority Ownership in Part. Proposing SBCs that are more than 50% owned by multiple venture capital operating companies (VCOC), hedge funds (HF), private equity firms (PEF), or any combination of these as set forth in 13 C.F.R. § 121.702, **are eligible** to submit proposals in response to DON topics advertised within this BAA.

For proposing SBCs that are a member of this ownership class the following must be satisfied for proposals to be accepted and evaluated:

a. Prior to submitting a proposal, SBCs must register with the SBA Company Registry Database.
b. The proposing SBC within its submission must submit the Majority-Owned VCOC, HF, and PEF Certification. A copy of the SBIR VC Certification can be found on https://navysbir.com/links_forms.htm. Include the SBIR VC Certification in the Supporting Documents (Volume 5).
c. Should a proposing SBC become a member of this ownership class after submitting its proposal and prior to any receipt of a funding agreement, the proposing SBC must immediately notify the

Contracting Officer, register in the appropriate SBA database, and submit the required certification, which can be found on https://navysbir.com/links_forms.htm.

System for Award Management (SAM). It is strongly encouraged that proposing SBCs register in SAM, https://sam.gov, by the Close date of this BAA, or verify their registrations are still active and will not expire within 60 days of BAA Close. Additionally, proposing SBCs should confirm that they are registered to receive contracts (not just grants) and the address in SAM matches the address on the proposal. An SBC selected for an award MUST have an active SAM registration at the time of award or they will be considered ineligible.

Cybersecurity Maturity Model Certification (CMMC) Program. DoW has established the CMMC Program to verify that awardees have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). CMMC Level requirements are identified within each topic and must be met prior to award. Proposing SBCs should anticipate that a Projected CMMC Level for Phase II award may be higher than the Projected CMMC Level advertised in the Phase I topic. Proposing SBCs should carefully review and consider the CMMC requirements as compliance may impact proposed costs and technical approach. Please review the DoW SBIR/STTR Program BAA for additional information on the CMMC Program.

Notice of NIST SP 800-171 Assessment Database Requirement. The purpose of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is to protect Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. As prescribed by DFARS 252.240-7997, in order to be considered for award, an SBC is required to implement NIST SP 800-171 and shall have a current assessment uploaded to the Supplier Performance Risk System (SPRS) which provides storage and retrieval capabilities for this assessment. The platform Procurement Integrated Enterprise Environment (PIEE) will be used for secure login and verification to access SPRS. For brief instructions on NIST SP 800-171 assessment, SPRS, and PIEE, please visit https://www.sprs.csd.disa.mil/nistsp.htm. For in-depth tutorials on these items, please visit https://www.sprs.csd.disa.mil/webtrain.htm.

Human Subjects, Animal Testing, and Recombinant DNA. Due to the short timeframe associated with Phase I of the SBIR/STTR process, the DON does **not** recommend the submission of Phase I proposals that require the use of Human Subjects, Animal Testing, or Recombinant DNA. For example, the ability to obtain Institutional Review Board (IRB) approval for proposals that involve human subjects can take 6-12 months, and that lengthy process can be at odds with the Phase I goal for time-to-award. Before the DON makes any award that involves an IRB or similar approval requirement, the proposing SBC must demonstrate compliance with relevant regulatory approval requirements that pertain to proposals involving human, animal, or recombinant DNA protocols. It will not impact the DON's evaluation, but requiring IRB approval may delay the start time of the Phase I award and if approvals are not obtained within two months of notification of selection, the decision to award may be terminated. If the use of human, animal, and recombinant DNA is included under a Phase I or Phase II proposal, please carefully review the requirements at: https://www.nre.navy.mil/work-with-us/how-to-apply/compliance-and-protections/research-protections. This webpage provides guidance and lists approvals that may be required before contract/work can begin.

Government Furnished Equipment (GFE). Due to the typical lengthy time for approval to obtain GFE, it is recommended that GFE is not proposed as part of the Phase I proposal. If GFE is proposed, and it is determined during the proposal evaluation process to be unavailable, proposed GFE may be considered a weakness in the technical merit of the proposal.

International Traffic in Arms Regulation (ITAR). For topics indicating ITAR restrictions or the potential for classified work, limitations are generally placed on disclosure of information involving topics of a classified nature or those involving export control restrictions, which may curtail or preclude the involvement of universities and certain non-profit institutions beyond the basic research level. Small businesses must structure their proposals to clearly identify the work that will be performed that is of a basic research nature and how it can be segregated from work that falls under the classification and export control restrictions. As a result, information must also be provided on how efforts can be performed in later phases if the university/research institution is the source of critical knowledge, effort, or infrastructure (facilities and equipment).

SELECTION, AWARD, AND POST-AWARD INFORMATION

Notifications. Email notifications for proposal receipt (approximately one week after the Phase I BAA Close) and selection are sent based on the information received on the proposal Cover Sheet (Volume 1). Consequently, the e-mail address on the proposal Cover Sheet must be correct.

Debriefs. Requests for a debrief must be made within 15 calendar days of select/non-select notification via email as specified in the select/non-select notification. Please note debriefs are typically provided in writing via email to the Corporate Official identified in the proposal of the proposing SBC within 60 days of receipt of the request. Requests for oral debriefs may not be accommodated. If contact information for the Corporate Official has changed since proposal submission, a notice of the change on company letterhead signed by the Corporate Official must accompany the debrief request.

Protests. Interested parties have the right to protest in accordance with the procedures in FAR Subpart 33.1.

Pre-award agency protests related to the terms of the BAA must be served to: osd.ncr.ousd-r-e.mbx.SBIR-STTR-Protest@mail.mil. A copy of a pre-award Government Accountability Office (GAO) protest must also be filed with the aforementioned email address within one day of filing with the GAO.

Protests related to a selection or award decision should be filed with the appropriate Contracting Officer for an Agency Level Protest or with the GAO. Contracting Officer contact information for specific DON Topics may be obtained from the DON SYSCOM Program Managers listed in Table 2 above. For protests filed with the GAO, a copy of the protest must be submitted to the appropriate DON SYSCOM Program Manager and the appropriate Contracting Officer within one day of filing with the GAO.

Awards. Due to limited funding, the DON reserves the right to limit the number of awards under any topic. Any notification received from the DON that indicates the proposal has been selected does not ultimately guarantee an award will be made. This notification indicates that the proposal has been selected in accordance with the evaluation criteria and has been sent to the Contracting Officer to conduct compliance review of Volume 3 to confirm eligibility of the proposing SBC, and to take other relevant steps necessary prior to making an award.

Contract Types. A Firm Fixed Price (FFP), Basic Ordering Agreement (BOA), or Prototype Other Transaction (OT) may be used for Phase I awards.

Funding Limitations. In accordance with the SBIR and STTR Policy Directive section 4(b)(5), there is a limit of one sequential Phase II award per SBC per topic. The maximum Phase I proposal/award amount including all options (including TABA) is $315,000. The Phase I Base amount must not exceed $200,000 and the Phase I Option amount must not exceed $115,000. The maximum Phase II proposal/award amount including all options (including TABA) is $2,000,000 (unless non-SBIR/STTR funding is being added). Individual SYSCOMs may award amounts, including Base and all Options, of less than

$2,000,000 based on available funding. The structure of the Phase II proposal/award, including maximum amounts as well as breakdown between Base and Option amounts will be provided to all Phase I awardees either in their Phase I award or a minimum of 30 days prior to the due date for submission of their Initial Phase II proposal.

Contract Deliverables. Contract deliverables for Phase I are typically a kick-off brief, progress reports, and a final report. Required contract deliverables (as stated in the contract) must be uploaded to https://www.navysbirprogram.com/navydeliverables/.

Payments. The DON makes three payments from the start of the Phase I Base period, and from the start of the Phase I Option period, if exercised. Payment amounts represent a set percentage of the Base or Option value as follows:

Days from Start of Base Award or Option	Payment Amount
15 Days	50% of Total Base or Option
90 Days	35% of Total Base or Option
180 Days	15% of Total Base or Option

Transfer Between SBIR and STTR Programs. Section 4(b)(1)(i) of the SBIR and STTR Policy Directive provides that, at the agency's discretion, projects awarded a Phase I under a BAA for SBIR may transition in Phase II to STTR and vice versa.

PHASE II GUIDELINES

Evaluation and Selection. All Phase I awardees may submit an **Initial** Phase II proposal for evaluation and selection. The evaluation criteria for Phase II is the same as Phase I (as stated in this BAA). The Phase I Final Report and Initial Phase II Proposal will be used to evaluate the SBC's potential to progress to a workable prototype in Phase II and transition the technology to Phase III. Details on the due date, content, and submission requirements of the Initial Phase II Proposal will be provided by the awarding SYSCOM either in the Phase I contract or by subsequent notification.

Awards. The DON will consider the following for Phase II award: Cost Plus Fixed Fee (CPFF), Firm Fixed Price (FFP), Basic Ordering Agreement (BOA), or Prototype Other Transaction (OT). Phase II awards can be structured in a way that allows for increased funding levels based on the project's transition potential. To accelerate the transition of SBIR/STTR-funded technologies to Phase III, especially those that lead to Programs of Record and fielded systems, the Commercialization Readiness Program was authorized and created as part of section 5122 of the National Defense Authorization Act of Fiscal Year 2012. The statute set-aside is 1% of the available SBIR/STTR funding to be used for administrative support to accelerate transition of SBIR/STTR-developed technologies and provide non-financial resources for the SBCs (e.g., the Navy SBIR Transition Program, STP).

Navy SBIR Transition Program (STP). Phase II awardees have the opportunity to participate in the virtual Navy STP Kickoff during the first or second year of the Phase II contract. While there are no travel costs associated with this virtual event, Phase II awardees should budget time of up to a full day to participate. STP information can be obtained at: https://navystp.com. Phase II awardees will be contacted separately regarding this program.

PHASE III GUIDELINES

A Phase III SBIR/STTR award is any work that derives from, extends, or completes effort(s) performed under prior SBIR/STTR funding agreements, but is funded by sources other than the SBIR/STTR programs. This covers any contract, grant, or agreement issued as a follow-on Phase III award or any

contract, grant, or agreement award issued as a result of a competitive process where the awardee was an SBIR/STTR firm that developed the technology as a result of a Phase I or Phase II award. The DON will give Phase III status to any award that falls within the above-mentioned description. Consequently, DON will assign SBIR/STTR Data Rights to any noncommercial technical data and noncommercial computer software delivered in Phase III that were developed under SBIR/STTR Phase I/II effort(s). Government prime contractors and their subcontractors must follow the same guidelines as above and ensure that companies operating on behalf of the DON protect the rights of the SBIR/STTR firm.

NAVY SBIR DoW 2026 BAA
Topic Index
Release 3

DON26BZ03-NV054 TITLE: Long-Range Listening Device

COMPONENT TECHNOLOGY PRIORITY AREA(S): Microelectronics;Sustainment

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

OBJECTIVE: Develop and demonstrate a long-range listening device capable of accurately identifying and recording sounds at a distance.

DESCRIPTION: Counterintelligence and Human Intelligence (CI/HUMINT) Marines perform intelligence operations in support of Marine Air-Ground Task Force (MAGTF) operations, with a focus on the collection of information and identification of threats posed by hostile organizations, espionage, sabotage, subversion, or terrorism. They require organic, portable capabilities to aid in the collection of information for intelligence reporting to decision makers. The capability to surveil sounds from a distance enhances their toolset. While long-range listening devices exist, innovation is required to meet the Marine Corps' portability, range, target area, accuracy, and recording requirements.
This SBIR topic seeks a small device that can accurately identify and record sounds at a distance.
Requirements for the Long-Range Listening Device
- Capable of effectively identifying and recording sounds at a distance of 200m (Threshold), while maintaining a minimal terminal target area of no more than 2 meters (Threshold).
- Capture and deliver sufficient recorded sound quality and target precision (at range) for a human listener to reliably differentiate voice, mechanical noises, and natural sounds such as wind and water.
- Small enough for an individual person to transport (50lbs or less) and set up from transit case to operational within one hour.
- Non-military in appearance (preferred).
- Able to operate by battery power with a minimum continuous recording time of 24 hours.

PHASE I: Design a concept for a long-range listening device that can meet the performance and size constraints listed in the Description. Demonstrate and validate the feasibility of the concept. Prepare a Phase II development plan with performance goals, key technical milestones, and risk reduction approaches.

PHASE II: Produce prototype hardware for a long-range listening device based on the Phase I work and requirements in the Description. Demonstrate and validate prototype performance in a realistic operational environment.

PHASE III DUAL USE APPLICATIONS: Though the primary objective is to support the Marine Corps to transition to support CI/HUMINT and force protection operations for the MAGTF. The other military Services and federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), Secret Service, and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), are likely to adopt this capability for similar long range surveillance operations. State and local law enforcement and private investigators could also employ the capability for surveillance.

REFERENCES:
1. Fluitt, Kim, et al. "Auditory Perception in Open Field: Distance Estimation." Army Research Lab, July 2013. https://www.researchgate.net/publication/301504471_Auditory_perception_in_open_field_Distance_estimation
2. Fluitt, Kim, et al. "Auditory Perception in an Open Space: Detection and Recognition." Army Research Lab, June 2015.

https://www.researchgate.net/publication/301502948_Auditory_perception_in_an_open_space_etection_and_recognition
3. Training and Education Command, US Marine Corps. "Marine Corps Reference Publication (MCRP) 2-10A.2, Counterintelligence and Human Intelligence." Quantico, VA: US Marine Corps, February 2025). https://www.marines.mil/Portals/1/Publications/MCRP%20210A.2%20(SECURED).pdf?ver=NgVh3ByQV9uNRbF3RnJQxA%3d%3d

KEYWORDS: Listening; Long-Range; Audio; Counterintelligence; Human Intelligence; Intelligence

DON26BZ03-NV055 TITLE: Multi-Band Approach to Target Discovery

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Quantum and Battlefield Information Dominance (Q-BID)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Space Technology

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a target discovery multi-band approach tool for wide-area ocean surveillance, target tracking, and environmental monitoring, to improve operational effectiveness and national security posture.

DESCRIPTION: Commercial Synthetic Aperture Radar (SAR) providers prioritize high-resolution imagery for applications demanding detailed ground sampling, primarily done in the X-band. This focus caters to markets like agriculture, urban planning, and disaster response. The Navy has a unique need for wide-area maritime surveillance, particularly in the open ocean, for tasks like search and rescue, tracking surface vessels, and monitoring illegal activities. The Navy also has urgent operational requirements for improved maritime domain awareness and more efficient resource allocation. Currently other methods are being used to perform these tasks; however, utilizing SAR would increase capabilities at a lower cost while providing better services for accomplishing the desired tracking methods. The Navy seeks a solution to utilize advancements in commercial space technology by utilizing dual-band SAR. Currently there is not a way for the Navy to utilize these services.

Dual-band approaches offer substantial benefits across various sectors. Dual-band routers and mobile devices can operate on both 2.4 GHz and 5 GHz frequencies, providing greater bandwidth and network capacity within telecommunications. This technology allows devices to switch to less congested frequencies, improving network performance and reliability in areas with high Wi-Fi density. Dual-band approaches can be used to monitor various environmental parameters, such as soil moisture, snow cover, and water quality, allowing for more accurate land cover classification and identification of specific features like vegetation types or mineral deposits. Within the medical field, dual-band imaging techniques can provide more detailed information about tissue composition and bone density, improving diagnostic capabilities for conditions like osteoporosis. Additionally, this approach can be used to enhance target detection and identification by combining data from different frequencies.
The solution sought will add to the current capabilities of searching, tracking, and monitoring to include dual-band SAR systems.

The system will incorporate a secondary band like S-band or C-band alongside the existing X-band capabilities. The system will increase area coverage and use lower frequency bands (S-band or C-band) that have wider beamwidths, enabling larger swaths of ocean to be imaged in a single pass. The increase in area coverage provided by a multi-band approach is not directly quantifiable with a single number as it is highly dependent on the specific bands used, the sensor technology, the platform, and the application.

Rather than a percentage increase, it is more accurate to discuss the types of coverage improvements that multi-band approaches offer, such as wider swath width, increased temporal coverage, and coverage in different domains. The benefits will be realized through the synergistic combination of different bands, each contributing unique information and capabilities.

The system must also have improved target detection through utilizing multiple frequencies that will allow for comprehensive target characterization. Different bands interact differently with various materials and sea states, enabling better discrimination among vessels, ice, and ocean features.
The dual-band SAR will provide enhanced environmental monitoring by providing valuable data for oceanographic applications, such as wave height and direction estimation, current monitoring, oil spill detection, flood monitoring, land cover classification, and sea ice monitoring.

Dual-Band performance validation will be accomplished through:

1. Frequency Band Coverage: Verification of operation within the specified frequency bands. Data will include spectral analysis in each band.
2. Simultaneous Operation: Demonstration of concurrent and independent operation in both frequency bands. Data will include recordings of simultaneous signal reception and processing in each band. Interference Mitigation: Assessment of the system's ability to mitigate interference between the two bands and from external sources. Data will include measurements under various interference conditions in each band.

Area Coverage Enhancement will be shown through:

1. Field of View (FOV) Measurement: Quantification of the increased FOV achieved by the dual-band approach compared to a single-band baseline system. Data will include geometric measurements and visualizations of the detectable area.
2. Detection Range: Determination of the maximum detection range in each band and in dual-band mode. Data will include plots of detection probability versus range for various target types and environmental conditions.
3. Target Tracking Accuracy: Evaluation of the system's ability to accurately track targets within the expanded FOV. Data will include measurements of target position error and tracking stability.
4. Open Ocean Search and Tracking Performance will be shown through:
Simulated Search Scenarios: Testing of the prototype in simulated open ocean environments with representative targets and clutter. Data will include detection and tracking performance metrics for various scenarios.
5. Environmental Impact Assessment: Evaluation of the system's performance under varying environmental conditions. Data will include performance metrics under different environmental parameters.

Prototype Robustness and Reliability will be shown through:

1. System Stability: Assessment of the system's stability and reliability during extended operation. Data will include continuous operation logs and failure rate analysis.
2. Power Consumption: Measurement of the system's power consumption under various operating conditions.

Navy Requirements Compliance will be shown through:

1. Specific Performance Metrics: Testing against specific Navy-defined performance metrics. Data will include direct measurements and comparisons to the required values. Performance specifications will be provided during Phase I.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National

Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a dual-band SAR and demonstrate through modeling and analysis that it feasibly meets the parameters in the Description. The Phase I Option, if exercised, will include the initial design specifications and capability to build a prototype solution in Phase II.

PHASE II: Develop a prototype dual-band SAR based on the results of Phase I. Demonstrate that the prototype meets parameters of the Description. Support Government testing at a Government-provided facility to determine the capability meets the performance goals of Navy. Deliver the prototype to the Navy.
It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use, which will include scaling up production and integrating with existing Navy systems.
Integrate the dual-band SAR system with Navy systems by collaborating with the Commercial Space Program Office (CSPO), integrating dual-band SAR data into workflows, creating software and algorithms that allow for effective processing and target detection, and provide personnel with training and support for interpreting data.

The objective is to secure long-term contracts with the Navy to provide ongoing access to dual-band SAR data/services with the benefit of marketing the technology to other government agencies in the future. To obtain successful commercialization and production, the performer will refine and optimize the prototype based on the Navy's testing and feedback from Phase II and set up manufacturing processes to produce the dual-band SAR system(s) at scale. This is valuable for applications like airport security, border surveillance, and traffic monitoring. The underlying principle is that using two or more frequency bands allows systems to leverage the unique characteristics of each band, enhancing performance, reliability, and overall capabilities.

REFERENCES:

1. Prabha, R. and Pandian, S.C. "Design and analysis of metamaterial inspired multiband, high gran superstrate patch antenna for military applications, WiMAX, and maritime mobile services." Optical and Quantum Electronics, Vol 56, Article Number 234, 2024 (Published 27 December 2023). https://link.springer.com/article/10.1007/s11082-023-05962-8#Abs1
2. Ouchi, Kazuo and Yoshida, Takero. "On the Interpretation of Synthetic Aperture Radar Images of Oceanic Phenomena: Past and Present." Remote Sens. 2023, 15, 1329. https://doi.org/10.3390/rs15051329 https://www.mdpi.com/2072-4292/15/5/1329
3. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Multi-band approach; Synthetic Aperture Radar; Open Ocean Search; Ocean Surveillance; Track Targets from space; Emitting Tracking Methods

DON26BZ03-NV056 TITLE: Optimizing Satellite Imagery across Commercial Vendors

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Quantum and Battlefield Information Dominance (Q-BID)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Integrated Network Systems-of-Systems;Space Technology

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a software application that uses a hub and spoke-style negotiating service for commercial satellite data providers (i.e., Imagery Synthetic Aperture Radar/ and Research and Development (SAR/RD)), utilizing their native Application Programming Interfaces (APIs) to forecast collection opportunities while optimizing resolution, speed of collection, and cost across multiple providers.

DESCRIPTION: Satellite imagery provides a critical foundation for maritime domain awareness (MDA), allowing the Navy to monitor vast ocean expanses, track vessel movements, and detect unusual activities while also supporting intelligence gathering by providing visual confirmation of suspected activities, revealing adversary capabilities and intentions, and informing strategic decision-making. The Navy primarily relies on its own dedicated reconnaissance assets and a limited number of Government contractors to receive imagery from satellites, which limits the speed of imagery reception and imposes reliance issues on accurate resources. A solution to the limiting factors would be to expand resources to multiple commercial satellite vendors, thus diversifying the sources of information and reducing reliance on single points of failure. The Navy seeks resilience in contested environments where access to a single vendor might be disrupted by weather or other conditions by development of an advanced hub and spoke-style scheduling optimization capability that will forecast opportunities and provide optimizing resolution, speed of collection, and costs across multiple commercial satellite providers. No known commercial capability can meet this need.
The solution application tool must provide a way to combine the following parameters.

1. It must achieve seamless multi-vendor integration that can be used for accessing a single, unified system and dynamically adapt to weather conditions by integrating real-time weather data and predictive models directly into the scheduling process.
2. It must also provide a prioritization capability for time-critical requirements such as tracking a high-value target or responding to a developing crisis.
3. It will optimize cost-efficiency for the scheduling process by selecting the most cost-effective vendor for a given task.
4. It will minimize redundant collections.
5. It will leverage opportunities for data sharing and collaboration among the commercial satellites.
6. It will enhance data fusion and analysis by combining imagery from different sources.
7. It must ensure data security and integrity by incorporating security measures.

The solution will be tested and must meet the following parameters:

1. System Functionality and Performance: includes integration testing, automated tasking and re-tasking, scalability and load testing, and user interface and functionality.
2. Imagery Quality and Usability: includes image resolution and clarity, cloud cover and obstruction analysis, and data fusion and processing.
3. Operational Effectiveness: includes simulated scenarios, field demonstrations, and user feedback/evaluation.
4. Security and Interoperability: includes security testing and interoperability testing.
5. Cost-Effectiveness Analysis: includes cost modeling and analysis.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a software hub and spoke-style scheduling optimization capability that feasibly meets the requirements in the Description. Demonstrate feasibility through modeling and analysis. The Phase I Option, if exercised, will include the initial design specifications and capabilities to build a prototype solution in Phase II.

PHASE II: Develop a prototype software hub and spoke-style scheduling optimization capability. Demonstrate that the prototype meets the parameters in the Description. Support testing of the prototype at a facility provided by the Government to determine it meets the required performance goals as stated in the Description. Deliver the prototype to the Navy.

It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use. Assist in testing the capability in the Government test facilities to ensure that the system meets the demanding requirements of the Maritime Targeting Cell-Afloat/Expeditionary (MTC-A/X) program and provides for future development and deployment decisions, ultimately contributing to a more effective and responsive imagery acquisition capability.

Outside of the military, this technology has the potential to revolutionize various sectors, such as law enforcement, marine wildlife protection, climate change research, vessel collision avoidance, supply chain management, coordination of rescue/relief efforts, and meteorology. The system could be deployed across multiple domains, improving safety, efficiency, and environmental protection in diverse environments.

REFERENCES:

1. Defence Geospatial Intelligence DGI). “DGI 2015 Industry Survey.” The 11th Annual Geospatial Intelligence Conference & Exhibition, 2015. http://dgi.wbresearch.com/media/1001380/27235.pdf
2. Cho, Doo-Hyun; Kim, Jun-Hong; Choi, Han-Lim and Ahn, Jaemyung. “Optimization-Based Scheduling Method for Agile Earth-Observing Satellite Constellation.” American Institute of Aeronautics and Astronautics, Journal of Aerospace Information Systems, November 2018, pp. 611-669. https://arc.aiaa.org/doi/epdf/10.2514/1.I010620
3. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Commercial satellite imagery; hub and spoke-style scheduling; speed of imagery reception; multi-vendor integration; single points of failure; data sharing and collaboration

DON26BZ03-NV057 TITLE: Gun Weapon Systems Ammunition Handling and Controls Modernization

COMPONENT TECHNOLOGY PRIORITY AREA(S): Human-Machine Interfaces; Microelectronics; Sustainment

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop an electro-mechanical capability for the sustained tactical loading and unloading of 5-inch/54 caliber naval ammunition.

DESCRIPTION: A component of both terminal defense and land-attack missions, a MK 34 GWS with the increased reliability and firing rates are expected to increase capability and survivability during missions in contested areas with large (10+) threat swarms. In these scenarios, the effective firing of ammunition to engage targets is essential due to relatively low-cost and on-hand inventory of shipboard ammunition (versus missiles).

Major Caliber Naval Gun Weapon Systems currently cycles conventional ammunition from storage conditions up through firing by way of circa-1960s electro-hydraulic power technology. With a high power-to-weight ratio and simple control circuits, this technology (militarized from the chemical and food machinery industry of the day) transformed ammunition handling systems from a manual to a semi-automated process aboard Navy ships.

The technology is old and has limitations on guided ammunition handling that include high maintenance requirements, obsolescence, complex troubleshooting, exposure to petroleum products, high intensity noise, and sustained operation limited by operator “in-the-loop” actions. There is currently no commercial technology that could solve the need for gun weapon systems ammunition handling and controls modernization for the Navy.

The Navy seeks a solution to modify existing fielded MK 34 Major Caliber Gun Weapon System guns (utilizing the MK 45 MOD 2 & 4 5-Inch Gun System) with automated ammunition loading systems that provide higher reliability (i.e., operational availability of .9 or greater), increased sustained loading (i.e., firing) rate (i.e., greater than 12 rounds per minute), and/or reduced exposure to occupational exposure to petroleum-based hydraulic fluids.

Potential innovations may incorporate electric motor drive technology, industrial control systems or testing system technologies, human-assist technologies, or process optimization. The solution shall be restricted to the MK 45 Gun System Size, Weight, and Power (SWaP) profile, requiring no modification to the platform (i.e., ship). All solutions shall utilize Model-Based Engineering (MBE) design principles. Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating

procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for an ammunition loading system for the MK 45 Gun System that meets the parameters in the Description. Establish feasibility through modeling and analysis of the design. The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype based on Phase I results. Demonstrate that the prototype will meet the requirements in the Description for each unique area of application within the Gun System. Install the prototype in a Government land-based test Gun System for testing and evaluation. Deliver the prototype to the Navy.

It is possible that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in successfully transitioning the technology to Navy use directly to both in-service and new production MK 45 5-inch Gun Mounts, the main component within the MK 34 Gun Weapon System aboard U.S. Navy Destroyers.
Upon successful transition of this R&D effort to the MK 34 GWS, other military applications of this technology include smaller caliber Gun Weapon Systems (20mm to 57mm). Non-military applications of this technology include industrial operations that require complex material handling and storage, including but not limited to, the automotive industry.

REFERENCES:

1. Al Bashar, Mahboob; Abu Taher, Md and Ashrafi, Dilara. “Enhancing Efficiency of Material Handling Equipment in Industrial Engineering Sectors.” IRE Journals, Volume 7 Issue 11, May 2024. https://www.researchgate.net/publication/380977469_Enhancing_Efficiency_of_Material_Handling_Equipment_in_Industrial_Engineering_Sectors
2. Khargonekar, Pramod P. and Dahleh, Munther A. “Advancing systems and control research in the era of ML and AI.” Annual Reviews in Control, Volume 45, 2018. https://www.sciencedirect.com/science/article/abs/pii/S1367578818300269
3. Hughes, Austin and Drury, Bill. “Electric Motors and Drives.” Elsevier Ltd., Oxford, United Kingdom: Newnes, 2019. https://archive.org/details/hughesa.druryb.electricmotorsanddrives.fundamentalstypesandapplications5ed2019
4. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Gun Weapon System; Conventional Ammunition; Guided Ammunition Handling; Major Caliber; Automated Ammunition Loading; Ammunition Handling System

DON26BZ03-NV058 TITLE: High-Throughput Embarked Data Transfer

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Quantum and Battlefield Information Dominance (Q-BID)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Advanced Computing and Software;Integrated Network Systems-of-Systems

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a small form factor device (total stowed volume of one cubic foot, including transceiver) and any required software to enable high-throughput data package transmission off embarked Navy platforms.

DESCRIPTION: U.S. Naval platforms defended by the Ship Self-Defense System (SSDS) combat management system (CMS) routinely traverse hostile regions of the world threatened by modern anti-ship weapons. SSDS CMS data recorded at sea are transmitted from embarked platforms back to various ashore support organizations for system performance analysis. Results are used in a variety of ways, which include but are not limited to improving CMS functionality, updating tactics, techniques, and procedures (TTPs), and ensuring warfighters are trained to defend platforms against modern threats in difficult scenarios. However, providing timely system improvements and guidance depends on timely receipt of large volumes of data for analysis. Existing methods of transmitting these data can be slow and bandwidth constrained, potentially reducing the cadence of this process and delaying the provision of important information.

The Navy seeks a small form factor device (total stowed volume of one cubic foot, including transceiver) and any required software to enable high-throughput data package transmission from embarked Navy platforms. The solution must transmit at least four terabytes of data in 60 seconds (i.e., at a sustained bandwidth of about 67GB/s) over more than 5,000 nautical miles. Currently no Commercial Off-the-Shelf (COTS) solutions are available for use in this manner.
Three SSDS Top Level Requirements (TLRs) are necessary.

- (U) The SSDS Combat System (CS) shall enable extraction of selected data for analysis and playback. [SSDS_CS_TLR-1041]
- (U) The SSDS CS shall provide extracted and recorded data for external processing. [SSDS_CS_TLR-1039]
- (U) The SSDS CS shall provide a method of updating its reference databases on a periodic basis, or on demand. [SSDS_CS_TLR-1207]

While modern techniques in radio, microwave, free space optical (FSO), or other data transmission modalities capable of satisfying these requirements are welcome, proposed solutions must be resilient to highly dynamic and challenging atmospheric or environmental effects on selected modalities and/or waveforms. Additionally, solutions must be capable of deployment on Navy surface combatants in fewer

than ten minutes from stowed to transmission ready. Solutions should plan to accept data from COTS data storage devices, including removable disk drives, removable Flash-based storage, and written optical media. Solutions must also be able to integrate with Department of War (DoW) Program of Record (PoR) communications architecture(s). The solution should provide technical details and clearly map those details to desired capability needs. The architecture should also provide high-level details regarding integration with DoW PoR communications architecture(s) or system(s), and should be designed and implemented in accordance with relevant DoW cybersecurity and information assurance (IA) standards. Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a small form factor device to enable high-throughput data package transmission and demonstrate feasibly that it meets all the requirements of the Description. Demonstrate feasibility of this concept to meet the conditions outlined in the Description through modeling, analysis, event-driven simulation of software capabilities, or other methods. The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype small form factor device to enable high-throughput data package transmission and any required software capabilities that enable integration with the DOW PoR communications architecture(s) based on the results of Phase I. Demonstrate that the prototype meets the required parameters in the Description. Support testing by the Government in a relevant environment provided by the Government. Deliver a prototype to the Navy.

It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use through system integration and qualification testing. Deliver the technology to support an IWS 80 critical test conducted jointly by the performer and the combat system engineering agent (CSEA), which is expected to take place on a surface combatant equipped with SSDS CMS software, demonstrating the full end-to-end data transmission process between the surface combatant and a Government ashore analysis and support activity.

Dual-use applications to consider include extension of these technologies and capabilities to expeditionary or remote use cases where exceptionally high throughput data package transmissions are required, including but are not limited to disaster recovery and relief, remote research and scientific operations such as polar science missions, and time-critical marine monitoring and regulatory oversight efforts.

REFERENCES:

1. Bath, W. G. “Overview of Platforms and Combat Systems.” Johns Hopkins APL Technical Digest, Vol. 35, No. 2, 2020. https://www.jhuapl.edu/Content/techdigest/pdf/V35-N02/35-02-Bath.pdf
2. Massachusetts Institute of Technology Lincoln Laboratory. “TeraByte InfraRed Delivery (TBIRD).” Innovation Highlight Technical Report, 2022. https://www.ll.mit.edu/sites/default/files/other/doc/2025-03/TTO_Technology_Highlight_12_TBird_2025.pdf
3. Boroson, Don M. et al. “A New Optical Communication Architecture for Delivering Extremely Large Volumes of Data from Space to Ground.” Proceedings of the AIAA SPACE 2015 Conference and Exposition, 28 August 2015. https://arc.aiaa.org/doi/10.2514/6.2015-4658
4. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004
5. Department of Defense Instruction (DODINST) 8500.01, “Cybersecurity.” Department of Defense Chief Information Officer. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
6. Department of Defense Instruction (DODINST) 8510.01, “Risk Management Framework (RMF) for DoD IT. Department of Defense Chief Information Officer. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf
7. National Institutes of Standards and Technology (NIST) SP 800-53, “Security and Privacy Controls for Information Systems and Organizations.” https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

KEYWORDS: Free space optical; FSO; data transmission modalities; challenging atmospheric or environmental effects; High-Throughput Data Package Transmission; Combat Management System; CMS; Tactics, Techniques, and Procedures; TTPs

DON26BZ03-NV059 TITLE: Real-time Zero Trust Data and Access Control for Combat Systems

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Integrated Sensing and Cyber

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a real-time Zero Trust data access control system for combat systems.

DESCRIPTION: The Navy relies on combat system data for critical decision-making in wartime. This data must be secure to prevent unauthorized access and ensure its integrity. Current security measures are struggling to keep up with evolving threats, making it difficult to guarantee data is only seen by authorized personnel. This vulnerability compromises tactical advantages and risks operational effectiveness. Traditional security approaches are often too slow and inflexible for the dynamic nature of modern naval operations. An answer to this need is not commercially available.
The Navy seeks an adaptive "Zero Trust" data control system. Zero Trust is a security strategy for modern multi-cloud networks. Instead of focusing on the network perimeter, a Zero Trust security model enforces security policies for each individual connection between users, devices, applications and data.
Zero Trust operates on the principle of “never trust, always verify” rather than granting implicit trust to all users inside a network. This granular security approach helps address the cybersecurity risks posed by remote workers, hybrid cloud services, personally-owned devices, and other elements of today’s networks. This goes beyond simply having usernames and passwords. The Navy needs to verify every data access request in near real time, regardless of the user's location or device.
The sought solution requires leveraging both Government and commercial technologies: Advanced Authentication - moving beyond passwords to biometrics, multi-factor authentication, and behavioral analysis; Micro-segmentation - dividing data into smaller highly-controlled compartments to limit the impact of any potential breach (think of it like having separate locked filing cabinets for different types of sensitive information); Artificial Intelligence (AI) and Machine Learning (ML) - detecting anomalous behavior and automatically adapting security measures, which could involve analyzing user access patterns to identify potential threats in real-time; and Blockchain Technology - exploring its potential for secure data logging and access control, ensuring an immutable record of all data transactions.
This Zero Trust system must ensure that only authorized personnel can access sensitive data, regardless of location or device type, which is crucial for maintaining a tactical advantage in future conflicts where information superiority will be paramount. Existing, new, and emerging technologies will be crucial in building this system.

While promising technologies exist, they are not currently integrated or robust enough to meet the Navy's stringent security requirements. The new system must address real-time performance and must ensure access verification suitable for fast-paced combat scenarios. The Navy requires near-instantaneous system access to effectively respond to dynamic and evolving threats.

Furthermore, scalability and integration with complex Navy networks and systems must be ensured, along with system resilience to cyberattacks and the ability to function in degraded environments (i.e., situations where critical infrastructure or communication links may be compromised due to enemy action, natural disasters, or other disruptive events). The solution must develop faster (reduce average authentication time from 15 seconds to 5 seconds) and more efficient authentication methods; implement micro-segmentation techniques to reduce the attack surface by dividing a network into smaller isolated security segments; integrate AI/ML for real-time threat detection and response; and explore and adapt blockchain technology for secure data management. The Navy aims to achieve significant improvements compared to existing systems, including reducing access latency by at least 50%, reducing the risk of unauthorized data access by at least 90%, and streamlining data management processes to reduce administrative overhead by at least 25%.

The developed technology will be evaluated against National Institute of Standards and Technology (NIST) standards for compartmented data control, cybersecurity and data integrity (e.g., NIST SP 800-207, Zero Trust Architecture).

The Navy requires the development and integration of an adaptive "Zero Trust" data control system to secure critical combat data. This system must leverage advanced authentication, micro-segmentation, and AI/ML to provide near real-time, verified access for authorized personnel across any device or location. Key performance requirements include reducing authentication time to under five seconds, decreasing the risk of unauthorized data access by at least 90%, and ensuring the system is scalable, resilient in degraded environments, and compliant with NIST standards.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a real-time Zero Trust data access control system for combat systems, specifically addressing the NIST standards associated with compartmented data control. Demonstrate the feasibility of this concept by providing detailed system architecture, including key technologies, algorithms, and data flow diagrams, which must include modeling and simulation to show the system's potential to meet Navy performance goals in the Description. (Note: If modeling and simulation alone cannot sufficiently demonstrate feasibility for specific aspects of the concept, propose and justify the use of subscale prototypes or surrogate systems, outlining their required characteristics and how they will contribute to a comprehensive feasibility assessment. For example, a subscale prototype might demonstrate the performance of a novel authentication mechanism under simulated network conditions, while a surrogate system could represent a simplified version of a combat system component for integration testing.)

The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype of the Zero Trust data access control system for combat systems based on the results of Phase I. Demonstrate the core functionalities of the proposed system, including authentication, authorization, micro-segmentation, and real-time threat detection. Support testing of the prototype in a representative environment mirroring the complexity and data flow of a combat system network and including simulated cyberattacks and operational scenarios to assess the system's resilience and performance under stress. Deliver the prototype to the Navy.

It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use. Transition the prototype Zero Trust data access control system into a fully operational capability for Navy use within the Maritime Targeting Cell - Afloat/Expeditionary (MTC-A/X) platform. The final product will be a robust, scalable, and secure system capable of managing and controlling access to sensitive combat system data in real-time, adhering to NIST standards and achieving the performance improvements outlined in previous phases.

The core technology developed under this effort has significant potential for dual-use applications in various commercial sectors. The need to protect sensitive data is not unique to the military. Businesses across numerous industries, including finance, healthcare, and energy, face similar challenges in safeguarding proprietary information and customer data from cyber threats and unauthorized access. The Zero Trust security model developed for the Navy can be adapted to protect sensitive corporate data, such as financial records, intellectual property, and personal health information.

REFERENCES:

1. Rose, S., Borchert, O., Mitchell, S. and Connelly, S. “Zero Trust Architecture, Special Publication (NIST SP).” National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420
2. Freter, Robert and the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team. “Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0.” July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
3. National Security Agency. “Embracing a Zero Trust Security Model Version 1.0.” February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
4. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Zero Trust Architecture; Access Control; Data Integrity; Cybersecurity; Multi-factor Authentication; Micro-segmentation

DON26BZ03-NV060 TITLE: Intra-Satellite Communications

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Quantum and Battlefield Information Dominance (Q-BID)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Space Technology

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a hardware capability that communicates rapidly between any commercial satellites to reduce latency of data transmission to track open ocean targets.

DESCRIPTION: The current model for commercial satellite communication involves each satellite independently communicating directly with ground stations or geostationary relay satellites. This architecture presents a significant challenge for tracking mobile targets, especially across wide areas. Because satellites do not communicate directly with each other, a target moving out of the field of view (FOV) of one satellite requires a time-consuming handoff process involving ground stations. This process introduces latency and inefficiencies, especially when trying to coordinate tracking across multiple satellites, whether from the same constellation or different vendors.
The use of existing commercial satellite infrastructure could provide the capability to mitigate these latencies and inefficiencies without the substantial cost of developing and deploying a dedicated military satellite network.

The Navy seeks a hardware solution to be installed on Government satellites that enables inter-satellite communication (ISC) within commercial satellite constellations. No existing commercial capability can accomplish this requirement. This proposed capability will allow satellites to directly share tracking data and other information and significantly improve the tracking of open ocean targets.
The solution must meet the following parameters:

1. Use Seamless Target Handoff to enable real-time communication between satellites, allowing for seamless tracking of objects as they move across the coverage areas of different satellites, eliminating the need for ground station intervention.
2. Use enhanced Tracking Accuracy and Persistence to direct communication between satellites.
3. Enable faster and more accurate correlation of target data from multiple viewpoints compared to the current time it takes to establish these same parameters.
4.Improve tracking accuracy, particularly for maneuvering targets.
5. Ensure persistent tracking even in challenging environments.
6. Establish an inter-satellite linked network that creates a dynamic and responsive network that adapts to changing operational needs.
7. Enable satellites to quickly share information about new targets or changes in target behavior, enhancing overall situational awareness.
8. Allow direct communication between satellites to reduce the time currently required to transmit critical tracking data to decision-makers.

9. Measure the data transfer latency between satellites under various network load and orbital configurations, as compared to latency experienced with traditional ground-relay communication systems.
10. Evaluate the data throughput capacity of the inter-satellite links and provide a determination of the maximum data rate that can be reliably sustained between satellites.
11. Assess the stability and reliability of the inter-satellite links under operational conditions for distances between satellites and atmospheric interference.
12. Test the effectiveness of routing data efficiently between satellites and route the data according to the most efficient routing protocol to achieve the most efficient routing between satellites, thus managing network congestion.
13. Improve target tracking accuracy achieved by using ISC compared to the accuracy using traditional methods with improved accuracy over the traditional methods. (Note: A baseline of traditional methods will be established to measure against an improvement provided by the solution, which must include the ability to measure the latency and message fidelity efficiency and seamlessness of target handoff between satellites including any associated loss of tracking data.)
14. Provide for assessing the coverage area of interest (AOI) footprint within the satellite pass and provide a determination of the ability of the network to maintain continuous tracking of targets moving across large areas.
15. Capable of simultaneously tracking multiple targets in accordance with the Commander's intent, including targets with varying speeds and trajectories.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for an intra-satellite communication hardware capability. Demonstrate feasibility through modeling and simulation showing the parameters in the Description can be achieved. Compare the cost of implementing and operating the intra-satellite communication system to the cost of alternative solutions, such as reliance solely on ground-based tracking systems. Assess the return on investment (ROI) achieved by leveraging commercial satellite infrastructure and implementing intra-satellite communication. The Phase I Option, if exercised, will include the initial design specifications and capabilities to build a prototype solution in Phase II.

PHASE II: Develop a prototype intra-satellite communication hardware capability based on the results of Phase I. Demonstrate that the prototype meets the parameters in the Description and the performance goals of Navy requirements. Support the Navy's comprehensive testing to validate the effectiveness of the system using evaluation metrics to quantify the system's performance. Deliver the prototype to the Navy. It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology for use in a wartime environment to track objects of interest. Assist the Navy in testing the technology's performance in actual conditions, which must be validated by demonstrating that the system meets the demanding requirements of modern naval operations via system integration and interoperability via operational testing in simulated scenarios and field testing.

Once operations of the system have provided feedback on its usability, effectiveness, and suitability for operational needs, the system will be used to inform future development and deployment decisions, ultimately providing concrete evidence of the system's capabilities and its potential to transform naval operations.

Outside the military, this technology has the potential to revolutionize various sectors, such as law enforcement, marine wildlife protection, vessel collision avoidance, supply chain management, coordination of rescue/relief efforts, and meteorology and space. The system could be deployed across multiple domains, improving safety, efficiency, and environmental protection in diverse environments.

REFERENCES:

1. Wang, Lixiang; Ye, Dong; Kong, Xianren and Xiao, Yan. "Adaptive multi-segment pseudospectral sequential convex programming for satellite cluster reconfiguration trajectory optimization." Advances in Space Research, Volume 75, Issue 8, 15 April 2025, pp. 6317-6341. https://doi.org/10.1016/j.asr.2025.01.072
2. Bakhsh, Zohre Mashayekh; Omid, Yasaman; Chen, Gaojie; Kayhan, Farbod; Ma, Yi and Tafazolli, Rahim. "Multi-Satellite MIMO Systems for Direct User-Satellite Communications: A Survey." arXiv preprint. June 2024, Cornell University, June 2024. IEEE Communications Surveys & Tutorials, Vol. X, No. X, XXX. https://arxiv.org/abs/2407.00196
3. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Data transfer latency; inter-satellite links; Tracking Accuracy and Persistence; geostationary relay satellites; data throughput capacity; target tracking accuracy; inter-satellite communications; ISC; intra-satellite communication

DON26BZ03-NV061 TITLE: Predictive Movement for Object Oriented Tracking

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Trusted AI and Autonomy

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a capability using Artificial Intelligence (AI) that investigates, tracks, and assigns priority for future state forecasting such as Geospatial-temporal Pattern of Life Analysis and change detection for the Maritime Targeting Cell (MTC).

DESCRIPTION: Maritime Targeting Cell is a high-tech "fusion" node, which receives massive amounts of data from diverse sources (e.g., satellites, sensors), making it difficult to process and interpret effectively. Current tracking relies heavily on manual methods, which can overwhelm staff and lead to inefficient resource allocation. They are essentially trying to find the proverbial needle in a haystack. Without an automated system, it is difficult to prioritize which objects require immediate attention, which can lead to critical threats being overlooked.

The Maritime Targeting Cell has a need to increase readiness for potential conflicts with adversaries. There are currently a large number of objects that need to be tracked, both above and below the surface of the ocean, across the globe. These objects include U.S. Navy Ships, other U.S. Government vessels, allied and partner Naval vessels, commercial vessels, adversary vessels, U.S. and other nations' submarines, underwater drones and sensors, and aircraft. The Navy needs to utilize efficient tracking methods for large numbers of objects so future state forecasting, pattern of life, and change detection can enable analysts to investigate targets, maintain track custody, and assign priority to objects detected.

As more sensors come online, the data volume will only increase, exacerbating existing problems. The current manual processes simply cannot scale and as the Navy's specific requirements are unique and complex, off-the-shelf tracking software is insufficient. Currently no existing commercial technology can meet this need.

The Navy envisions an AI-driven solution that aims to address these challenges by automating key aspects of the tracking process.

The solution must meet the following parameters:

1. It must use AI-powered tracking algorithms to process sensor data, identify and track objects, and predict their future movements.
2. It must use Automated Prioritization in which AI is used for activity prediction and Pattern of Life (POL) analysis to assign a priority level to each tracked object, allowing analysts to focus on the most important targets first.
3. It must use Predictive Forecasting and Change Detection to analyze historical data and current behavior and predict future object states and quickly identify deviations from expected patterns, enhancing situational awareness.

4. It must contain Hierarchical Target Management to allow the system to maintain track custody of all objects, but present them to analysts in a prioritized hierarchy, allowing for efficient resource allocation.
5. It will need to have Enhanced Scalability so as new sensors are added, the AI can seamlessly integrate the additional data without requiring a proportional increase in manpower.
6. It will need to have Improved Response Time through automating analysis and prioritization to accelerate the decision-making process, enabling faster responses to developing situations.

In essence, the proposed AI solution aims to transform the Navy from a reactive overwhelmed center to a proactive highly efficient hub for maritime domain awareness, which will empower the Navy to better manage the vast amount of data it collects and make more informed decisions, ultimately enhancing national security.

Evaluation metrics will be used to quantify the system's performance, including accuracy, precision, recall, F1-score (a balanced measure of precision and recall), processing time, false positive rate, and false negative rate. These metrics will measure how often the system correctly identifies and tracks objects, the proportion of correctly identified objects out of all identified and all actual objects, a balance of precision and recall, the data processing time, and the rates of incorrect object identification and missed object identification.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for an AI-driven maritime tracking system that automates data processing, object identification and tracking, and threat prioritization. Demonstrate the feasibility of this concept through modeling and simulation, showing how the proposed algorithms can achieve the required levels of accuracy in object identification, tracking, and prioritization using simulated sensor data representing realistic maritime scenarios. Ensure that this simulation demonstrates (1) the concept's ability to handle increasing data loads that reflect the Navy's future needs, (2) improved response times compared to current manual methods, and (3) the feasibility of hierarchical target management to prioritize objects based on predicted threat level. (Note: While full prototypes are not expected in Phase I, performers might need to develop subscale prototypes or surrogates of specific AI modules, such as predictive forecasting or POL analysis components.)

The Phase I Option, if exercised, will include the initial design specifications and capabilities to build a prototype solution in Phase II.

PHASE II: Develop a prototype AI-driven maritime tracking tool based on the results of Phase I. Demonstrate the core functionalities of the prototype, including AI-driven tracking, prioritization, predictive forecasting and change detection, hierarchical target management, enhanced scalability, and improved response time. Support rigorous prototype testing using simulated and/or real-world maritime

sensor data and evaluation on the performance against metrics defined in the Description, including accuracy, prioritization effectiveness, and response time improvement. (Note: If a full prototype is cost-prohibitive, advanced modeling and simulation using representative data can be used to demonstrate the technology's potential.) Ensure that the prototype meets key requirements including specified accuracy levels, prioritization thresholds, and demonstrable improvements in response time and scalability.
It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use. Support testing to ensure that the system meets the demanding requirements of modern naval operations via operational testing in simulated scenarios and field testing to assess its performance in actual conditions.

Once operators of the system have provided feedback on its usability, effectiveness, and suitability for operational needs, the system will be used to inform future development and deployment decisions, ultimately contributing to an enhanced scalability and improved response time.
Outside of the military, this technology has the potential to revolutionize various sectors, such as law enforcement, marine wildlife protection, climate change research, vessel collision avoidance, supply chain management, coordination of rescue/relief efforts, and meteorology. The system could be deployed across multiple domains, improving safety, efficiency, and environmental protection in diverse environments.

REFERENCES:

1. Haldorai, Anandakumar; Lincy, R. Babitha; Suriya, M.; Balakrishnan, Minu. “Enhancing Military Capability Through Artificial Intelligence: Trends, Opportunities, and Applications.” Springer Nature Link. April 2024, pp. 359-370. https://doi.org/10.1007/978-3-031-53972-5_18
2. Bellagamba, Laurence; Patterson, Stuart; Biber, Klaus; Pirolo, David and Ewart, Roberta M. “Science and Technology Roadmaps to Enhance Military Space System Resilience.” AIAA Space 2016, Los Angeles, California, 13-16 September 2016. https://doi.org/10.2514/6.2016-5473
3. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Pattern of Life; Hierarchical Target Management node; predictive forecasting; object oriented tracking; Change Detection; Automated Prioritization

DON26BZ03-NV062 TITLE: Secure Tasking of Commercial Assets

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Contested Logistics Technologies (LOG)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Integrated Sensing and Cyber; Space Technology

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a capability for intercommunication between Government and commercial satellites.

DESCRIPTION: Maritime Targeting Cell-Afloat/Expeditionary (MTC-A/X)'s purpose is to provide weapons-quality tracks to support over-the-horizon targeting by using multi-intelligence capabilities across all domains and deliver direct sensor data downlink capability. To maintain a tactical advantage, the Navy requires the ability to task commercial satellites at Controlled Unclassified Information (CUI)/Information Level-5 (IL-5) and Secret Level (IL-6) to ensure tasking is not discoverable by adversaries.

The Navy could task commercial satellites for missions requiring secure handling of sensitive information, like targeting; however, commercial satellite providers typically do not offer the security levels required for classified Government operations [CUI impact levels (IL)-5 or Secret IL-6]. They could modify existing military systems for commercial use but that is prohibitively expensive and impractical for commercial vendors. Nothing that is commercially available can fulfill this communications need.

The Navy needs a capability to securely task commercial satellites at the required classification levels. This requires a solution leveraging both Government and commercial technologies, such as implementing end-to-end encryption within existing commercial tasking interfaces, secure data transfer protocols, and blockchain-based solutions for verifying the authenticity and integrity of tasking requests. The performer must evaluate the feasibility of integrating commercial security technologies like secure cloud platforms and Virtual Private Networks (VPNs) and explore emerging technologies such as quantum-resistant cryptography for enhanced long-term security.

The solution must establish a baseline for data security with an initial focus on establishing secure methods for tasking commercial satellites at the required CUI levels. Subsequent efforts will focus on solutions that demonstrate measurable reductions in tasking latency - measuring the speed and efficiency of the tasking process, verifying a targeted 90% reduction in tasking time compared to current methods, for which standard tasking can take up to 14 days from order to delivery. Seamless integration across different cybersecurity requirements will further contribute to more timely tasking, increased tasking opportunities, and a stronger overall cybersecurity posture.

The developed technology will be evaluated in a simulated environment against National Institute of Standards and Technology (NIST) standards for secure communications and data handling at the specified classification levels. This performer will also leverage existing Navy contracts, such as those managed by the Commercial Space Program Office (CSPO), to ensure rapid transition and widespread adoption across the DoW.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a secure satellite tasking system that meets the parameters in the Description. Demonstrate the feasibility of this concept by providing a detailed concept design, including system architecture, security protocols, integration plans with existing commercial tasking interfaces, and modeling and simulation to show the system's potential to meet Navy performance goals in the Description. (Note: If modeling and simulation alone cannot sufficiently demonstrate feasibility for specific aspects of the concept, propose and justify the use of simulations or subscale demonstrations to illustrate key aspects of the concept, particularly related to security and integration. For example, a simulation demonstrating the secure transfer of encrypted tasking data between a mock commercial interface and a simulated secure government network would be beneficial.)
Specify the number and delivery schedule of any prototype articles provided to the Government for testing in the Phase II SOW based on the specific approach proposed by the performer.
The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype secure satellite tasking system based on the results of Phase I. Demonstrate the core functionality of the secure tasking system, including secure communication channels, data encryption/decryption, authentication and authorization mechanisms, and integration with representative commercial tasking interfaces.
(Note: If full prototype development is deemed too costly within the Phase II budget, the contractor may propose alternative evaluation methods, such as detailed simulations or analytical modeling, to demonstrate the prototype meets Navy performance goals. These alternative methods must be clearly justified and provide sufficient evidence to support the claims.
It is probable that the work under this effort will be classified under Phase II (see Description section for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the secure satellite tasking system to operational use within the Navy. The prototype will be developed and integrated within the Maritime Targeting Cell program and seamlessly integrated with commercial satellite providers. Support the transition process by refining and hardening the system: addressing any remaining bugs or vulnerabilities identified during Phase II testing and optimizing performance for operational use; developing comprehensive documentation and training materials to provide Navy personnel with the

necessary resources to operate and maintain the system effectively; providing ongoing technical support; and assisting the Navy with system integration, deployment, and troubleshooting.
While developed for military applications, this secure satellite tasking technology has significant potential for dual use in the commercial sector. Many industries rely on satellite imagery but face challenges protecting sensitive or proprietary information. This technology could be adapted to provide secure tasking and data transfer for secure commercial applications and safeguard proprietary information from unauthorized access. Other potential applications include precision agriculture to protect sensitive crop data from competitors; environmental monitoring to secure data related to pollution or resource exploration; and urban planning to protect sensitive infrastructure information.

REFERENCES:

1. Enright, Kevin. “What is Satellite Tasking and How Does it Work?” UP42, 23 June 2022. https://up42.com/blog/what-is-satellite-tasking-and-how-does-it-work
2. Morisse, Barry. “Simplifying the Process of Tasking a Satellite.” GEO AWESOME, 29 May 2024. https://geoawesome.com/eo-hub/simplifying-the-process-of-tasking-a-satellite/
3. Cloud Information Center. “Cloud Security.” https://cic.gsa.gov/basics/cloud-security
4. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Commercial Satellite Tasking; Blockchain-Based Authentication; End-to-End Encryption; satellite tasking classified information; Secure Data Transfer; Quantum-resistant cryptography

DON26BZ03-NV063 TITLE: Anomalous Behavior Detection and Alerting for Congested Maritime Environments

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Human-Machine Interfaces; Trusted AI and Autonomy

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a capability for automated Pattern of Life (PoL) analysis in congested maritime environments.

DESCRIPTION: U.S. Navy platforms defended by the Ship Self-Defense System (SSDS) combat system frequently transit maritime regions of the world that are congested with oceangoing vessels and aircraft traffic, which may include fishing vessels, tankers and cargo container ships, commercial airliners, or hostile entities such as enemy surface combatants or anti-air warfare (AAW) threats. In those congested maritime environments, enemies may attempt to hide within the noise of maritime congestion in an effort to gain initiative and surprise against U.S. Navy forces. There are some information sources at the disposal of Ship's Force to detect adversaries. For example, both surface vessels (using Automatic Identification System (AIS) or aircraft (using Automatic Dependent Surveillance – Broadcast (ADS-B)) publicly broadcast certain types of information about themselves, including but not limited to Global Positioning System (GPS) location, speed, altitude, destination, and other identifying information as appropriate. However, not all regions have requirements that all traffic must broadcast this information, and actors conducting nefarious or illegal activity have been known to disable AIS and ADS-B systems on their craft. Non-cooperative methods to determine the intent of these craft have been developed in response to the risks posed by uncompliant vessels or aircraft, including PoL analysis. Here, longitudinal records of typical traffic patterns are established over time, then compared against real-time observations to identify anomalous – and therefore potentially nefarious or threatening – activity that is out of family from those records, such as deviation from established vessel traffic separation schemes (TSS), frequently-traveled flight paths or air corridors, or fishing activity in unexpected areas, among others. Anomalous contacts can then be flagged for increased scrutiny by human operators or other actions. However, detailed monitoring and analysis can be difficult for human operators and watchstanders to do for an entire transit duration or extended stay within a congested environment. For example, it requires close attention to detail over long periods of time, which can induce attentional fatigue and missed indicators by operators. Additionally, in the absence of digital historical records and/or when traversing new areas, Ship's Force may have no historical collective knowledge of maritime traffic patterns against which to compare observations. The safety-critical nature of this task, coupled with the challenge it poses for humans, suggests a unique and important target for automation. Currently no commercial answer to the problem exists.

The Navy seeks the capability to analyze PoL behaviors exhibited by nearby maritime traffic for various regions of the world. Solutions must comprehensively explore all traffic (surface and air) within a 360-degree coverage area around a notional ship, using one or more PoL methods to identify targets that are anomalous and potentially threatening to the ship. Solutions must leverage common sources of maritime traffic data and include at a minimum AIS, ADS-B, and notional air or surface contacts detected by notional radars; other data sources can be specified, but must be realistic for Navy ships to collect, then identify and describe. Tracks or conditions of interest identified by the system must generate alerts for operators via decision support systems or other capabilities that are developed alongside automated analysis and detection logic. Selected alerting content and methods are flexible, but at a minimum must include system track numbers, select descriptive details of the track, provide an explanation of the machine reasoning for the alert that was generated, and compile a machine confidence assessment of the conclusion.

Proposed solutions must (1) function without large volumes of historical traffic patterns and trends stored within the combat system's computers or databases, (2) include a notional plan for future integration with the SSDS combat system and its operator displays, and (3) be accompanied by an architecture that specifies at a minimum: sources of input data required for analysis; communications and/or data exchange pathways to support analysis needs; specific points of integration between algorithm(s) or method(s) used to perform PoL analysis and selected data sources; and operator alerting and information dissemination capabilities that could integrate with SSDS displays.

Proposals should address data volume concerns associated with storing large PoL databases and describe methods to execute the proposal without requiring significant additional data storage devices and without limiting PoL data to temporary "region-specific" data holdings that must be expunged as ship Operating Areas (OPAREAs) change.

Improved methods of automated PoL analysis that can identify potentially threatening sea or air contacts and communicate findings to watchstanders would significantly improve safety conditions for SSDS vessels transiting these regions.

Three SSDS Top Level Requirements (TLRs) would be supported by this investigation.

- The SSDS CS shall generate and display the [Common Tactical Picture] to support command situation awareness and combat coordination. [SSDS_CS_TLR-1222]
- The SSDS CS shall provide a means by which operators are notified and are able to participate in the resolution of identification conflicts. [SSDS_CS_TLR-1492]
- The SSDS CS shall determine ID and classification with whatever data is available. [SSDS_CS_TLR-1486]

Work should include contacts and composite track data that are produced organically by SSDS combat system sensors, as well as architectural updates that specify the methods or approaches by which PoL analysis will be performed using a fusion of maritime tracks and organic SSDS composite tracks. Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security

Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for an automated PoL analysis method in congested maritime environments meeting the requirements in the Description. Assess feasibility through modeling, simulation, or other means. Ensure that selected methods are explainable. The Phase I Option, if exercised, will include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype automated PoL analysis method in congested maritime environments. Demonstrate functionality and performance of a full 360-degree coverage capable of meeting realistic operational SSDS use cases and needs for specific regions, as well as a detailed plan for integrating this solution with SSDS. (Note: To support successful Phase II efforts, the Acquisition Office will provide information regarding the SSDS architecture, U.S. Navy consoles and display environment capabilities, and world regions of interest.) Deliver the prototype to the Navy.

It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use through system integration and qualification testing for the prototype hardware capability developed in Phase II. Deliver the prototype to support an IWS 80 critical experiment conducted jointly by the performer and the combat system engineering agent (CSEA), to take place in a live environment with tactical SSDS combat system software. (Note: The transition will require integration of the prototype into SSDS.)

Dual-use applications to consider include but are not limited to sea- or land-based private or third-party transportation, shipping, and logistics applications; personnel security; event security; and environmental and resource extraction regulatory monitoring.

REFERENCES:

1. Bath, W. G. “Overview of Platforms and Combat Systems.” Johns Hopkins APL Technical Digest, Vol. 35, No. 2, 2020. https://www.jhuapl.edu/Content/techdigest/pdf/V35-N02/35-02-Bath.pdf
2. Forti, N.; Millefiori, L. M. and Braca, P. “Unsupervised extraction of maritime patterns of life from Automatic Identification System data.” OCEANS 2019 - Marseille, Marseille, France, 2019, pp. 1-5. DOI: 10.1109/OCEANSE.2019.8867429
3. Ducruet, C. ed. “Maritime networks Spatial structures and time dynamics.” Routledge, 2015. https://www.taylorfrancis.com/books/edit/10.4324/9781315692852/maritime-networks-c%C3%A9sar-ducruet
4. Spiliopoulos, G.; Vodas, M.; Grigoropoulos, G.; Bereta, K, and Zissis, D. “Patterns of Life: Global Inventory for maritime mobility patterns.” Series ISSN: 2367-2005. EDBT, pp. 770-777, 2024. https://openproceedings.org/2024/conf/edbt/paper-216.pdf
5. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Maritime traffic; Pattern of Life Analysis; PoL; Automatic Identification System; AIS; Automatic Dependent Surveillance – Broadcast; ADS-B; System Track Numbers; Anomalous Contacts in congested maritime environments

DON26BZ03-NV064 TITLE: Terminal Defense Weapon System Coordinator

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Advanced Computing and Software; Integrated Network Systems-of-Systems; Trusted AI and Autonomy

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop a Terminal Defense System Weapon System Coordinator (TDSWC) for terminal defense system weapon system engagements.

DESCRIPTION: PEO IWS 11 is responsible for providing terminal defense weapon systems for ship self-defense against Anti-Ship Missile (ASM), Helicopter, Aircraft, Unmanned Aerial Systems (UAS), and Surface Threats. The program's portfolio includes Rolling Airframe Missile (RAM), Close-in Weapon System (CIWS), Counter-Unmanned Aircraft Systems (CUAS), Directed Energy, and Guns. Ship combat systems direct and manage terminal defense weapon system engagements so terminal defense weapon system upgrades require an update to the ship combat system. In addition, ship combat system weapon direction and management require complex algorithms in the ship combat system plus a detailed understanding of weapon systems' performance.

Ship combat system weapon system updates are part of the combat system's major releases. This takes years of development, followed by years of fielding.

The Navy seeks a capability that decouples weapon system upgrades from ship combat system updates and allows terminal defense systems to develop and field updates within two months. Currently no existing commercial technology can meet this need. The solution will move the ship combat system terminal defense weapon system responsibilities for managing upgrades and weapon system coordinating engagements from the combat system to the weapon system coordinator in real-time without latency. Development of the weapon system coordinator solution must use model-based system engineering (MBSE) for documenting requirements, developing the architecture, and testing the behavior. The coordinator shall use Artificial Intelligence (AI) for engagement coordination by implementing AI heuristics and machine learning. The MBSE model shall include a code generator that will translate the model to an executable program that can be run on a RED HAT LINUX platform. The coordinator will include a combat system interface for managing combat system commands as well as cyber secure interfaces to each terminal defense weapon system.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able

to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NASEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a TDSWC concept using MBSE. Demonstrate feasibility in meeting the weapon system coordinator requirements using modelling, simulation, and analysis. The Phase I Option, if exercised, will include the initial design specifications and a capabilities description to build a prototype in Phase II.

PHASE II: Develop a TDSWC prototype based on results of the Phase I. Demonstrate the prototype meets the Description parameters by integrating the executable software into a Navy-provided simulation testbed that complies with the combat system and terminal defense systems interface requirements. Verify the prototype meets the defined requirements and architectures. Deliver the prototype to the Navy.
It is probable that the work under this effort will be classified under Phase II.

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the prototype TDSWC model and executable to a Navy appointed warfare center for future development and maintenance. Provide oversight during the transition of the TDSWC. Assist the Navy in product field testing, implementing upgrades, and porting the executable to different computing platforms.
Successful use of MBSE to document requirements, architecture and executable is desirable for products that can be used on a variety of computing platforms. The design and behavior of the product remains the same while the implementation of the product changes based on the computing platform's characteristics (physical configuration, manufacturer, instruct set architecture, etc.). As such, this technology is useful for all computing architectures in corporations.

REFERENCES:

1. Mitchell, Steven W. "Model-based System Development for Managing the Evolution of a Common Submarine Combat System." A FCEA-GMU C4I Center Symposium on Critical Issues in C4I, 18-19 May 2010. STEVEMITCHELL_CI_C4I_2010V6. https://www.omg.org/sysml/Model_Based_Approach_to_Manage_Evolution-SteveMitchell_CI_C4I_2010v6.pdf
2. Lockheed Martin Company. "Lockheed Martin MDA Success Story: F16 Modular Mission Computer Application Software." Based on a presentation by Lauren E. Clark, Chief Engineer F-16 Modular Mission Computer Software; Terry Ruthruff, Staff Specialist Software Engineering Core; and Bary D. Hogan, Methodology Lead F-16 Modular Mission Computer Software. https://www.omg.org/mda/mda_files/LockheedMartin.pdf
3. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Ship Combat System; Model Based System Engineering; MBSE; Code Generator; Terminal Defense System; TDSWC; AI Heuristics; Weapon System Coordinating

DON26BZ03-NV065 TITLE: Adaptive Sensor Management

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Advanced Computing and Software; Integrated Sensing and Cyber

PROJECTED CMMC LEVEL REQUIREMENT: Level 2 (Self)

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Develop an algorithmic capability for dynamic resource allocation that characterizes existing Ship Self-Defense System (SSDS) sensor tasking allocations, the relative magnitude of each sensor's fire control data contributions to composite tracks, identify sensor resources that could be released for other more impactful tasking without sacrificing current track quality metrics of relevance, and specify existing or potentially new sensor tasking that would benefit most from re-allocation of those resources.

DESCRIPTION: Navy aircraft carriers and amphibious warfare (L-class) ships are defended by the SSDS, a combat system comprised of weapons, sensors, communications systems, computers, and other elements working together to detect, track, and engage inbound anti-ship missiles and other threats. SSDS platforms sense their environments and identify tracks of interest by integrating inputs from a variety of sensors, which include rotating, fixed face and fire control or target illumination radars that cover a variety of radar bands, as well as electronic support (ES) sensors that process received Radio Frequency (RF) waveforms. Each of these sensors provides its update to the combat system at different rates. For example, while phased array radars can provide rapid target measurements and schedule beams or dwells across a wide field of view, rotating radars may have much narrower fields of view (FOVs) and provide full rotations only once every several seconds. However, because each sensor strives to maximize performance and provide the information necessary for SSDS to build and maintain fire control quality tracks on targets of interest, there are conditions in which further aggregation of sensor data may provide diminishing returns related to fire control track quality (e.g., continuing to provide updates on certain well-characterized tracks may not offer significant track state covariance reductions or additional fire control quality improvements over its current state). It may be advantageous in these cases to shift some of those sensor tasks to other combat system needs, specifically where those additional tasks could substantially improve track quality on other targets or help improve situation awareness via other means. Nothing available commercially can provide this capability.

The Navy seeks an algorithm-based software solution that automatically detects which sensors are contributing to fire control quality tracks on particular targets, assesses the relative magnitudes of their contributions, identifies conditions in which particular sensor resources could be released for other sensor tasking, and specifies which current or potentially novel sensor tasking would benefit most from allocation of those released resources. Proposed solutions should be dynamic, adaptive, responsive to rapid changes in track hostility characterization (i.e., solvable in real-time or better, minimizing algorithmic worst-case time complexity), and work with heterogeneous combinations of sensor tasking

and resource utilization feedback parameters. Solutions must identify each sensor's capability that is controllable by SSDS (e.g., search sectors, search modes, track-based controls, and cueing capabilities, among others) and leverage those realistic features in a solution for SSDS.
Examples of alternative sensor tasking include but are not limited to: executing surface-, volume-, or sector-specific search patterns; modifying or updating search modes; applying track-based controls; cueing other sensors on a specific target; or other actions. Example algorithmic techniques and fields from which approaches could be derived include stochastic and Bayesian optimization, metaheuristics, model predictive control theory, or others. Proposals using artificial intelligence and machine learning approaches will also be considered, but proposers should note that candidate solutions must be capable of generating resource re-allocation recommendations in scenarios that may be completely novel to the combat system and for which little to no prior exposure has been provided. Finally, proposed solutions should correspond to and be compatible with the existing SSDS Program of Record sensors. The initial solution will focus on mathematical and algorithmic development needed to address interactions between four radars that either are or will be installed on most SSDS platforms: SPS-48, SPQ-9B, MK-9 Tracker/Illuminator, and SPY-6(V)3. Solutions should be demonstrable under low to medium-fidelity modeling and simulation approaches, and the algorithmic solutions included in the proposed solution must be explainable.

Five SSDS Top Level Requirements (TLRs) would be supported by this investigation (note that, in the requirements language below, EW signifies Electronic Warfare, and ES signifies Electronic Support):

- The SSDS Combat System (CS) shall provide a sensor cueing capability that automatically selects and assigns air tracks to specified own ship sensors for the purpose of achieving requisite track confidence and track data quality to support automatic engagement recommendations at maximum range allowed by engagement doctrine. [SSDS_CS_TLR-289]
- The SSDS CS shall perform cued radar search for high-priority ES tracks that meet specified criteria but are not correlated or associated with existing SSDS CS active radar tracks. [SSDS_CS_TLR-291]
- The SSDS CS shall detect resource utilization conflicts between sensors and resolve them based on the sensor resource priorities established. [SSDS_CS_TLR-1300]
- The SSDS CS shall have automated and manual capabilities to request additional target EW data by ES sensor(s) for a specified track to support updates to EW classification. [SSDS_CS_TLR-1607]
- The SSDS CS shall coordinate above water radar activities based on radar capabilities, availability, and tactical and operational conditions. [SSDS_CS_TLR-1631]

Solutions explored during a potential Phase II award must include an expanded set of sensors, the last of which is an ES sensor. The full sensor suite will therefore include SPS-48, SPS-49, SPQ-9B, SPY-6(V)2, SPY-6(V)3, MK-9 Tracker/Illuminator, and SLQ-32(V)6.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVSEA in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Develop a concept for a dynamic resource allocation software capability that characterizes existing SSDS sensor task allocations and provides a solution that meets all requirements identified in the Description. Show feasibility of the concept using modeling, simulation, analysis, or other methods that are explainable, as well as references from sensor tracking and resource management open literature for resource management inputs. (Note: To support realistic demonstration and candidate solution development, the performer will be provided with a reference combat system architecture example and additional sensor tasking information.) Phase I solutions will be advisory in nature, where recommendations will be provided to sensor and/or combat system operators for evaluation and action. If the Phase I Option is exercised, include the initial design specifications and capabilities description to build a prototype solution in Phase II.

PHASE II: Develop a prototype dynamic resource allocation algorithm-based software capability that characterizes existing SSDS sensor tasking allocations based on the results of Phase I, expanding to include the Phase II sensors identified in the Description as well as SSDS-specific fire control quality tracking and sensor resource management details. Phase II will also include a trade study to explore overall system performance where resource allocation actions are automatically taken by the system vice made to human operators for consideration and possible action. (Note: Phase II will require a notional plan for integrating the product into the SSDS combat system.) Deliver the prototype to the Navy.
It is probable that the work under this effort will be classified under Phase II (see the Description for details).

PHASE III DUAL USE APPLICATIONS: Support the Navy in transitioning the technology to Navy use through system integration and qualification testing for the prototype hardware capability developed in Phase II. Deliver the prototype to support an IWS 80 critical experiment conducted jointly by the proposer and the combat system engineering agent (CSEA), expected to take place in a live environment with tactical SSDS combat management system (CMS) software. (Note: The transition will require integration of the prototype into the SSDS CMS.)

Dual-use applications to consider are self-driving cars, vehicles, and other platforms equipped with multiple sensors; manufacturing and production quality control systems; and other applications where systems must dynamically prioritize and allocate sensor coverage to maintain maximum system efficiency.

REFERENCES:

1. Bath, W. G. “Overview of Platforms and Combat Systems.” Johns Hopkins APL Technical Digest, Vol. 35, No. 2, 2020. https://www.jhuapl.edu/Content/techdigest/pdf/V35-N02/35-02-Bath.pdf
2. Li. Zhize et al., “Heterogeneous Sensing for Target Tracking: Architecture, Techniques, Applications and Challenges.” Measurement Science and Technology, Vol. 34, No. 7, pp. 1-25. https://iopscience.iop.org/article/10.1088/1361-6501/acc267/pdf
3. Li, Tianqi; Krakow, L.W. and Gopalswamy, S. “Optimizing Consensus-based Multi-target Tracking with Multiagent Rollout Control Policies.” 2021 IEEE Conference on Control Technology and Applications (CCTA), San Diego, CA, USA, 2021, pp. 131-137. doi: 10.1109/CCTA48906.2021.9658603. https://arxiv.org/pdf/2102.02919; https://ieeexplore.ieee.org/document/9658603
4. National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993). https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Target Illumination Radars; Sensor Resources; Dynamic Resource Allocation; Bayesian Optimization; Model Predictive Control Theory; Alternative Sensor Tasking