AMENDMENT 1

Defense Advanced Research Projects Agency (DARPA)
DoD 23.4 Small Business Innovation Research (SBIR) Annual BAA
Proposal Submission Instructions
Release 5

The purpose of Amendment 1 to DARPA Release 5 is to include programmatic changes as required by the SBIR and STTR Extension Act of 2022 (Pub. L. 117-183). Additional disclosure requirements are outlined in Appendix A, Supporting Documents (Volume 5)

INTRODUCTION

DARPA's mission is to make strategic, early investments in science and technology that will have long-term positive impacts on our national security. As part of this mission, DARPA makes high-risk, high-reward investments in science and technology that have the potential to disrupt current understandings and/or approaches. The pace of discovery in both science and technology is accelerating worldwide, resulting in new fields of study and the identification of scientific areas ripe for small business utilization through the SBIR and STTR programs. Small businesses are critical for developing technology to support national security. Proposers are encouraged to consider whether the R/R&D being proposed to DoD Components also has private sector potential, either for the proposed application or as a base for other applications. The topics below focus on technical domains important to DARPA's mission pursuing innovative research concepts that fall within one of its technology offices. More information about DARPA's technical domains and research topics of interest may be found at: http://www.darpa.mil/about-us/offices.

Proposers responding to a topic in this BAA must follow all general instructions provided in the Department of Defense (DoD) SBIR Program BAA. DARPA requirements in addition to or deviating from the DoD Program BAA are provided in the instructions below.

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

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

Specific questions pertaining to the administration of the DARPA Program and these proposal preparation instructions should be directed to: DARPA Small Business Programs Office at SBIR_BAA@darpa.mil.

DSIP Topic Q&A will NOT be available for these DARPA topics. Technical questions related to improving the understanding of a topic's requirements must be submitted to SBIR_BAA@darpa.mil by the deadline listed below.

The following dates apply to this DARPA Topic release:

April 27, 2023: Topics issued for pre-release
May 18, 2023: Topics open; DARPA begins accepting proposals via DSIP
June 08, 2023: Deadline for technical question submission
June 16, 2023: Deadline for receipt of proposals no later than **12:00 pm ET**

DIRECT TO PHASE II PROPOSAL GUIDELINES

Proposers should refer to the DARPA Direct to Phase II Proposal Instructions, provided in Appendix A.

Current Release Award Structure by Topic

Topic Number	Direct to Phase II				
	Tech Volume*	Award Amount	Period of Performance (PoP)	Option Amount	Option PoP
HR0011SB20234-08	35 pages	$600,000	10 months	N/A	N/A
HR0011SB20234-09	35 pages	$1,200,000	24 months	$600,000	12 months
HR0011SB20234-10	35 pages	$1,200,000	24 months	$600,000	12 months
HR0011SB20234-11	35 pages	$1,200,000	24 months	$600,000	12 months
HR0011SB20234-12	35 pages	$1,200,000	24 months	$600,000	12 months
HR0011SB20234-13	35 pages	$1,200,000	24 months	$600,000	12 months

Technical Volume (Volume 2) – Abbreviated Standard Format (35-page)
If a proposer can provide adequate documentation to substantiate that the scientific and technical merit and feasibility described in the Phase I section of the topic has been met and describes the potential commercial applications, the Direct to Phase II (DP2) authority allows the Department of Defense (DoD) to make an award to a small business concern under Phase II of the SBIR program without regard to whether the small business concern was provided an award under Phase I of an SBIR program. This topic is accepting DP2 proposal submissions.

DP2 Feasibility Documentation shall not exceed 10 pages. DP2 Technical Proposal shall not exceed 20 pages. Phase II commercialization strategy shall not exceed 5 pages. This should be the last section of the Technical Volume and will not count against the 30-page limit.

Content of the Technical Volume
Proposers should refer to the DARPA DP2 Proposal Instructions, provided in Appendix A and on the DARPA Small Business site (https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program).

Cost Volume (Volume 3)
Please see the chart above for award amounts listed by topic. Proposers are required to use the Direct to Phase II – Volume 3: Cost Proposal Template (Excel Spreadsheet) provided on the DARPA Small Business site (https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program).

NOTE: Subcontractors may also submit unsanitized cost proposals using this template directly to DARPA at SBIR-BAA@darpa.mil.

Please review the updated Percentage of Work (POW) calculation details included in the DoD Program BAA. DARPA will occasionally accept deviations from the POW requirements with a letter of explanation or approval from the Funding Agreement officer.

Company Commercialization Report (CCR) (Volume 4)
Completion of the CCR as Volume 4 of the proposal submission in DSIP is required. Please refer to the DoD SBIR Program BAA for full details on this requirement. Information contained in the CCR will not be considered by DARPA during proposal evaluations.

Supporting Documents (Volume 5)

In addition to the documents required by DoD, small businesses may also submit additional documentation to support the Technical Volume (Volume 2) and the Cost Volume (Volume 3) in Volume 5. See Appendix A for **required** certifications that must be included in Volume 5. For additional information, see the SBIR 23.4 Annual Program Broad Agency Announcement (BAA) at https://www.defensesbirsttr.mil/SBIR-STTR/Opportunities/.

DISCRETIONARY TECHNICAL AND BUSINESS ASSISTANCE (TABA)
DARPA does not offer TABA funding.

EVALUATION AND SELECTION
All proposals will be evaluated in accordance with the evaluation criteria listed in the DoD SBIR 2023.4 BAA. DARPA will conduct an evaluation of each conforming proposal. Proposals that do not comply with the requirements detailed in this BAA and the research objective(s) of the corresponding topic are considered non-conforming and therefore are not evaluated nor considered for award.

Using the evaluation criteria, the Government will evaluate each proposal in its entirety, documenting the strengths and weaknesses relative to each evaluation criterion, and, based on these identified strengths and weaknesses, determine the proposal's overall selectability. Proposals will not be evaluated against each other during the evaluation process, but rather evaluated on their own individual merit to determine how well the proposal meets the criteria stated in this BAA and the corresponding DARPA topic.

Awards will be made to proposers whose proposals are determined to be the most advantageous to the Government, consistent with instructions and evaluation criteria specified in the DoD SBIR 2023.4 BAA and availability of funding. Given the limited funding available for each topic released, not all proposals considered selectable will be selected for funding.

For the purposes of this proposal evaluation process, a selectable proposal is defined as follows:

Selectable: A selectable proposal is a proposal that has been evaluated by the Government against the evaluation criteria listed in the DoD SBIR 2023.4 BAA and DARPA topic, and the strengths of the overall proposal outweighs its weaknesses. Additionally, there are no accumulated weaknesses that would require extensive negotiations and/or a resubmitted proposal.

For the purposes of this proposal evaluation process, a non-selectable proposal is defined as follows:

Non-Selectable: A proposal is considered non-selectable when the proposal has been evaluated by the Government against the evaluation criteria listed in the DoD SBIR 2023.4 BAA and DARPA topic, and the strengths of the overall proposal do not outweigh its weaknesses.

Proposing firms will be notified of selection or non-selection status for a Phase I award within 90 days of the closing date of the topic. It is the policy of DARPA to treat all proposals as source selection information and to disclose their contents only for the purpose of evaluation. Restrictive notices notwithstanding, during the evaluation process, submissions may be handled by support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors are expressly prohibited from performing DARPA-sponsored technical research and are bound by appropriate nondisclosure agreements. Input on technical aspects of the proposals may be solicited by DARPA from other Government and/or non-Government consultants/experts who are strictly bound by the appropriate non-disclosure requirements. No submissions will be returned. Upon completion of the evaluation and selection process, an electronic copy of each proposal received will be retained at DARPA.

Proposal titles, abstracts, anticipated benefits, and keywords of proposals that are selected for contract award will undergo a DARPA Policy and Security Review. Proposal titles, abstracts, anticipated benefits, and keywords are subject to revision and/or redaction by DARPA. Final approved versions of proposal titles, abstracts, anticipated benefits, and keywords may appear on the DoD SBIR/STTR awards website and/or the SBA's SBIR/STTR award website (https://www.sbir.gov/sbirsearch/award/all).

Refer to the DoD SBIR 2023.4 Program BAA for procedures to protest the Announcement.
As further prescribed in FAR 33.106(b), FAR 52.233-3, Protests regarding the selection decision should be submitted to:

DARPA
Contracts Management Office (CMO)
675 N. Randolph Street
Arlington, VA 22203
E-mail: scott.ulrey@darpa.mil and sbir@darpa.mil

AWARD AND CONTRACT INFORMATION

1. General Award Information

Multiple awards are anticipated. DARPA may award FAR-based government contracts (Firm- Fixed Price or Cost-Plus Reimbursement) or Other Transactions for Prototypes agreement (under the authority of 10 U.S.C. § 4022) subject to approval of the Contracting Officer. The amount of resources made available for each topic issued under this BAA will depend on the quality of the proposals received and the availability of funds.

Majority Ownership in Part. Proposers 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 DARPA topics advertised within this BAA.

For proposers 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, firms must register with the SBA Company Registry Database.
b. The proposer 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://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program, under SBIR/STTR BAA Forms. Include the SBIR VC Certification in the Supporting Documents (Volume 5).
c. Should a proposer become a member of this ownership class after submitting its proposal and prior to any receipt of a funding agreement, the proposer must immediately notify the Contracting Officer, register in the appropriate SBA database, and submit the required certification which can be found under SBIR/STTR BAA Forms and Templates on https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program.

The Government reserves the right to select for negotiation all, some, one, or none of the proposals received in response to this announcement and to make awards with or without communications with proposers. Additionally, the Government reserves the right to award all, some, one, or none of the options on the contract(s)/agreement(s) of the performers based on available funding and technical performance. If warranted, portions of resulting awards may be segregated into pre-priced options. Additionally, DARPA reserves the right to accept proposals in their entirety or to select only portions of proposals for award. In the event that DARPA desires to award only portions of a proposal, negotiations may be opened

with that proposer. The Government reserves the right to fund proposals in phases with options for continued work, as applicable.

The Government reserves the right to request any additional, necessary documentation once it makes the award instrument determination. The Government reserves the right to remove a proposal from award consideration should the parties fail to reach agreement on award terms, conditions, and price within a reasonable time, and/or the proposer fails to provide requested additional information within three business days.

In all cases, the Government Contracting Officer reserves the right to select award instrument type, regardless of instrument type proposed, and to negotiate all instrument terms and conditions with selectees. DARPA will apply publication or other restrictions, as necessary, if it determines that the research resulting from the proposed effort will present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Any award resulting from such a determination will include a requirement for DARPA permission before publishing any information or results on the program. For more information on publication restrictions, see the DoD SBIR 2023.4 BAA.

Because of the desire to streamline the award negotiation and program execution process, proposals identified for negotiation will result in negotiating a type of instrument for award that is in the best interest of the Government. In the case of an OT for Prototype agreement under DARPA's authority to award OTs for prototype projects, 10 U.S.C. § 4022, use of an OT provides significant opportunities for flexible execution to assist in meeting DARPA's aggressive SBIR/STTR program goals.

All proposers that wish to consider an OT award should carefully read the following:

The flexibility of the OT award instrument is beneficial to the program because the Performer will be able to apply its best practices as required to carry out the research project that may be outside of the Federal Acquisition Regulation (FAR) process-driven requirements. Streamlined practices will be used, such as milestone-driven performance, intended to reduce time and effort on award administration tasks and permit performers to focus on the research effort and rapid prototyping. Because of this ability, OTs provide the Agreements Officer the flexibility to create an award instrument that contains terms and conditions that promote commercial transition, reduce some administratively burdensome acquisition regulations, and meet SBIR/STTR program goals.

Proposers must only propose an OT agreement with fixed payable milestones. Fixed payable milestones are fixed payments based on successful completion of the milestone accomplishments agreed to in the milestone plan. Refer to the Other Transactions for Prototypes Fact Sheet and Other Transaction for Prototype Agreement, available at https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program. Specific milestones will be based upon the research objectives detailed in the topic.

Please see https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program for more information on OTs.

2. Transition and Commercialization Support Program (TCSP)

DARPA will provide services to Phase II or DP2 awardees upon contract execution through the Transition and Commercialization Support Program (TCSP) at no cost to awardees. The TCSP goal is to maximize the potential for SBIR/STTR companies to move their technology beyond Phase II and into other research and development programs for further maturity or into solutions or products for DoD acquisition programs, other Federal programs, and/or the commercial market. Please visit

https://www.darpa.mil/work-with-us/for-small-businesses/commercialization-continued for more information on DARPA TCSP.

3. Embedded Entrepreneurship Initiative

Awardees of SBIR funding pursuant to this BAA may be eligible to participate in the DARPA Embedded Entrepreneurship Initiative (EEI) during the Period of Performance. Invitation to participate in EEI is at the sole discretion of the Government based on evaluation of technical and commercial factors and subject to program balance and the availability of funding. EEI is a limited scope program offered by DARPA, at DARPA's discretion, to a small subset of awardees. The goal of DARPA's EEI is to increase the likelihood that DARPA-funded technologies take root in the U.S. and provide new capabilities for national defense. EEI supports DARPA's mission "to make pivotal investments in breakthrough technologies and capabilities for national security" by accelerating the transition of innovations out of the lab and into new capabilities for the Department of Defense (DoD). EEI investment supports development of a robust and deliberate Go-to-Market strategy for selling technology product to the government and commercial markets and positions DARPA awardees to attract U.S. investment. The following is for informational and planning purposes only and does not constitute solicitation of proposals to the EEI.

There are three elements to DARPA's EEI: (1) A Senior Commercialization Advisor (SCA) from DARPA who works with the Program Manager (PM) to examine the business case for the awardee's technology and uses commercial methodologies to identify steps toward achieving a successful transition of technology to the government and commercial markets; (2) Connections to potential industry and investor partners via EEI's Investor Working Groups; and (3) Additional funding on an awardee's contract for the awardee to hire an embedded entrepreneur to achieve specific milestones in a Go-to-Market strategy for transitioning the technology to products that serve both defense and commercial markets. This embedded entrepreneur's qualifications should include business experience within the target industries of interest, experience in commercializing early stage technology, and the ability to communicate and interact with technical and non-technical stakeholders. Funding for EEI is typically no more than $250,000 per awardee over the duration of the award. An awardee may apportion EEI funding to hire more than one embedded entrepreneur, if achieving the milestones requires different expertise that can be obtained without exceeding the awardee's total EEI funding. The EEI effort is intended to be conducted concurrent with the research program without extending the period of performance.

EEI Application Process:

After receiving an award under the solicitation, awardees interested in being considered for EEI should notify their DARPA Program Manager (PM) during the period of performance. Timing of such notification should ideally allow sufficient time for DARPA and the awardee to review the awardee's initial transition plan, identify milestones to achieve under EEI, modify the award, and conduct the work required to achieve such milestones within the original award period of performance. These steps may take 9-18 months to complete, depending on the technology. If the DARPA PM determines that EEI could be of benefit to transition the technology to product(s) the Government needs, the PM will refer the performer to DARPA Commercial Strategy.

DARPA Commercial Strategy will then contact the performer, assess fitness for EEI, and in consultation with the DARPA technical office, determine whether to invite the performer to participate in the EEI. Factors that are considered in determining fitness for EEI include DoD/Government need for the technology; competitive approaches to enable a similar capability or product; risks and impact of the Government's being unable to access the technology from a sustainable source; Government and commercial markets for the technology; cost and affordability; manufacturability and scalability; supply chain requirements and barriers; regulatory requirements and timelines; Intellectual Property and Government Use Rights, and available funding.

Invitation to participate in EEI is at the sole discretion of DARPA and subject to program balance and the availability of funding. EEI participants' awards may be subsequently modified bilaterally to amend the Statement of Work to add negotiated EEI tasks, provide funding, and specify a milestone schedule which will include measurable steps necessary to build, refine, and execute a Go-to-Market technology transition plan aimed at delivering new capabilities for national defense. Milestone examples are available at: https://www.darpa.mil/work-with-us/contract-management.

Awardees under this solicitation are eligible to be considered for participation in EEI, but selection for award under this solicitation does not imply or guarantee participation in EEI.

For more information please refer to the EEI website https://eei.darpa.mil/.

4. DARPA Toolbox Initiative

DARPA Toolbox is an Agency-wide effort to provide open licensing opportunities with commercial technology vendors to the researchers behind DARPA programs. DARPA Toolbox provides easy, low-cost, scalable access to state-of-the-art tools and intellectual property (IP) under predictable legal terms and streamlined acquisition procedures. The goal is to reduce performer reliance on low-quality, low-cost tools and IP that increase execution risks and complicate post-DARPA transitions.

Through this initiative, DARPA performers are granted access to select vendor tools and technologies throughout the life of their contractual relationship with the Agency. The Toolbox suppliers bring to the table proven technologies commonly used in state-of-the art commercial microelectronics or system design methodologies.

DARPA Toolbox program information and a full list of participating suppliers can be found at https://www.darpa.mil/work-with-us/darpa-toolbox-initiative. If there are tool or technologies of interest, contact the Supplier POC listed for the product, referencing the DARPA Toolbox Initiative. The Supplier POC will provide advice on products and pricing information. Include any non-production pricing quotes in your proposal. Products and pricing are between you and the suppliers – *do not* contact DARPA directly.

ADDITIONAL INFORMATION

DARPA intends to use electronic mail for all correspondence regarding these topics. Questions related to the technical aspect of the research objectives and awards specifically related to a topic should be emailed to SBIR_BAA@darpa.mil. Please reference the topic number in the subject line. All questions must be in English and must include the name, email address, and the telephone number of a point of contact.

DARPA will attempt to answer questions in a timely manner; however, questions submitted within seven (7) calendar days of the proposal due date listed herein may not be answered. DARPA will post a consolidated Frequently Asked Questions (FAQ) document. To access the posting please visit: http://www.darpa.mil/work-with-us/opportunities. Under the topic number summary, there will be a link to the FAQ. The FAQ will be updated on an ongoing basis until one week prior to the proposal due date.

Technical support for the Defense SBIR/STTR Innovation Portal (DSIP) is available Monday through Friday, 9:00 a.m. – 5:00 p.m. ET. Requests for technical support must be emailed to DoDSBIRSupport@reisystems.com with a copy to SBIR_BAA@darpa.mil.

AMENDMENT 1

APPENDIX A: DARPA DIRECT TO PHASE II (DP2) PROPOSAL INSTRUCTIONS

I. Introduction

A complete proposal submission consists of:

Volume 1: Proposal Cover Sheet
Volume 2: Technical Volume (feasibility documentation and technical proposal)
Volume 3: Cost Volume
Volume 4: Company Commercialization Report
Volume 5: Supporting Documents
- a. Contractor Certification Regarding Provision of Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Attachment 1) MANDATORY
- b. Disclosures of Foreign Affiliations or Relationships to Foreign Countries (Attachment 2) MANDATORY
- c. Verification of Eligibility of Small Business Joint Ventures (Attachment 3), if applicable
- d. Disclosure of Funding Sources (Attachment 4) MANDATORY
- e. Other supporting documentation
- **A completed proposal submission in DSIP does NOT indicate that the mandatory supporting documents have been uploaded. It is the responsibility of the proposing small business concern to ensure that the mandatory documents listed above have been uploaded and included with the proposal submission.**

Volume 6: Fraud, Waste and Abuse Training

The Defense SBIR/STTR Innovation Portal (DSIP) provides a structure for building the proposal volumes and submitting a consolidated proposal package. If this is your first time submitting an SBIR or STTR proposal using DSIP, please review detailed training guides at https://www.dodsbirsttr.mil/submissions/learning-support/training-materials. It is the responsibility of the proposing firm to ensure that a complete proposal package is certified and submitted by the close date listed in the topic to which they are responding.

To assist in proposal development, templates for Volume 2: Technical Volume and Volume 3: Cost Volume have been provided as attachments to the announcement posted at https://www.dodsbirsttr.mil/submissions/login Use of these templates is mandatory.

NOTE: All proposers are required to submit Volume 4: Company Commercialization Report (CCR).

II. Proprietary Information

Proposers that include in their proposals data that they do not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes, shall follow instructions in section 4.5 regarding marking propriety proposal information.

III. DP2 Proposal Instructions

a. Proposal Cover Sheet (Volume 1)

The Cover Sheet must include a brief technical abstract of no more than 3000 characters that describes the proposed R&D project with a discussion of anticipated benefits and potential commercial applications.

Do not include proprietary or classified information in the Proposal Cover Sheet. If your proposal is selected for award, the technical abstract and discussion of anticipated benefits may be publicly released.

b. Format of Technical Volume (Volume 2) – standard format

1. The Technical Volume must include two parts, PART ONE: Feasibility Documentation (10 pages) and PART TWO: Technical Proposal (20 pages).

2. Type of file: The Technical Volume must be a single Portable Document Format (PDF) file, including graphics. Perform a virus check before uploading the Technical Volume file. If a virus is detected, it may cause rejection of the proposal. Do not lock or encrypt the uploaded file. Do not include or embed active graphics such as videos, moving pictures, or other similar media in the document.

3. Length: The length of each part of the technical volume (Feasibility Documentation and Technical Proposal) will be specified by the corresponding topic. The Government will not consider pages in excess of the page count limitations.

4. Layout: Number all pages of your proposal consecutively. Font size should not be smaller than 10-point on standard 8-1/2" x 11" paper with one-inch margins. The header on each page of the Technical Volume should contain your company name, topic number, and proposal number assigned by DSIP when the Cover Sheet was created. The header may be included in the one-inch margin.

c. Content of the Technical Volume (Volume 2) – Standard Format

PART ONE: Feasibility Documentation

1. Provide documentation to substantiate that the scientific and technical merit and feasibility described in the Phase I section of the topic has been met and describe the potential commercial applications. To be eligible, proposers must demonstrate that the feasibility requirements outlined in the topic have been met, and achieved outside of the SBIR program. Documentation should include all relevant information including, but not limited to: technical reports, test data, prototype designs/models, and performance goals/results.
2. Maximum page length for feasibility documentation will be specified by the topic. If you have references, include a reference list or works cited list as the last page of the feasibility documentation. This will count towards the page limit.
3. Work submitted within the feasibility documentation must have been substantially performed by the proposer and/or the PI.
4. If technology in the feasibility documentation is subject to Intellectual Property (IP), the proposer must either own the IP, or must have obtained license rights to such technology prior to proposal submission, to enable it and its subcontractors to legally carry out the proposed work. Documentation of IP ownership or license rights shall be included in the Technical Volume of the proposal.
5. Include a one-page summary on Commercialization Potential addressing the following:
   i. Does the company contain marketing expertise and, if not, how will that expertise be brought into the company?
   ii. ii. Describe the potential for commercial (Government or private sector) application and the benefits expected to accrue from this commercialization.

DO NOT INCLUDE marketing material. Marketing material will NOT be evaluated.

PART TWO: Standard Technical Proposal

Significance of the Problem. Define the specific technical problem or opportunity addressed and its importance.

1. Phase II Technical Objectives. Enumerate the specific objectives of the Phase II work, and describe the technical approach and methods to be used in meeting these objectives.
2. Phase II Statement of Work. The statement of work should provide an explicit, detailed description of the Phase II approach, indicate what is planned, how and where the work will be carried out, a schedule of major events and the final product to be delivered. The methods planned to achieve each objective or task should be discussed explicitly and in detail. This section should be a substantial portion of the total proposal.
    a. Human/Animal Use: Proposers proposing research involving human and/or animal use are encouraged to separate these tasks in the technical proposal and cost proposal in order to avoid potential delay of contract award.
    b. Phase II Option Statement of Work (if applicable, specified in the corresponding TOPIC). The statement of work should provide an explicit, detailed description of the activities planned during the Phase II Option, if exercised. Include how and where the work will be carried out, a schedule of major events and the final product to be delivered. The methods planned to achieve each objective or task should be discussed explicitly and in detail.

3. Related Work. Describe significant activities directly related to the proposed effort, including any conducted by the PI, the proposer, consultants or others. Describe how these activities interface with the proposed project and discuss any planned coordination with outside sources. The proposal must persuade reviewers of the proposer's awareness of the state of the art in the specific topic. Describe previous work not directly related to the proposed effort but similar. Provide the following: (1) short description, (2) client for which work was performed (including individual to be contacted and phone number) and (3) date of completion.

5. Relationship with Future Research or Research and Development.
    i. State the anticipated results of the proposed approach if the project is successful.
    ii. Discuss the significance of the Phase II effort in providing a foundation for Phase III research and development or commercialization effort.

6. Key Personnel. Identify key personnel who will be involved in the Phase II effort including information on directly related education and experience. A concise resume of the PI, including a list of relevant publications (if any), must be included. All resumes count toward the page limitation. Identify any foreign nationals you expect to be involved on this project.

7. Foreign Citizens. Identify any foreign citizens or individuals holding dual citizenship expected to be involved on this project as a direct employee, subcontractor, or consultant. For these individuals, please specify their country of origin, the type of visa or work permit under which they are performing and an explanation of their anticipated level of involvement on this project. Refer to section 3.2 of this BAA for more information. Supplemental information provided in response to this paragraph will be protected in accordance with the Privacy Act (5 U.S.C. 552a), if applicable, and the Freedom of Information Act (5 U.S.C. 552(b)(6)).

8. Facilities/Equipment. Describe available instrumentation and physical facilities necessary to carry out the Phase II effort. Items of equipment to be purchased (as detailed in the cost proposal) shall be justified under this section. Also state whether or not the facilities where the proposed work will be performed meet environmental laws and regulations of federal, state (name) and local Governments for, but not limited to, the following groupings: airborne emissions, waterborne effluents, external radiation levels, outdoor noise, solid and bulk waste disposal practices and handling and storage of toxic and hazardous materials.

9. Subcontractors/Consultants. Involvement of a university or other subcontractors or consultants in the project may be appropriate. If such involvement is intended, it should be identified and described according to the Cost Breakdown Guidance. Please refer to section 3 of this BAA for detailed eligibility requirements as it pertains to the use of subcontractors/consultants.

10. Prior, Current or Pending Support of Similar Proposals or Awards. If a proposal submitted in response to this topic is substantially the same as another proposal that was funded, is now being funded, or is pending with another Federal Agency, or another or the same DoD Component, you must reveal this on the Proposal Cover Sheet and provide the following information:
    a. Name and address of the Federal Agency(s) or DoD Component to which a proposal was submitted, will be submitted, or from which an award is expected or has been received.
    b. Date of proposal submission or date of award.
    c. Title of proposal.
    d. Name and title of the PI for each proposal submitted or award received.
    e. Title, number, and date of BAA(s) or solicitation(s) under which the proposal was submitted, will be submitted, or under which award is expected or has been received.
    f. If award was received, state contract number.
    g. Specify the applicable topics for each proposal submitted or award received.

Note: If this does not apply, state in the proposal "No prior, current, or pending support for proposed work."

11. Transition and Commercialization Strategy (5 pages). DARPA is equally interested in dual use commercialization of SBIR/STTR projects that result in products sold to the U.S. military, the private sector market, or both. DARPA expects explicit discussion of key activities to achieve this result in the transition and commercialization strategy part of the proposal. The Technical Volume of each Direct to Phase II proposal must include a transition and commercialization strategy section. The Phase II transition and commercialization strategy shall not exceed 5 pages, and will NOT count against the proposal page limit.

    Information contained in the commercialization strategy section will be used to determine suitability for participation in EEI. Selection for participation in EEI will be made independently following selection for SBIR/STTR award. Please refer to section 3 of the Instructions for more information on the DARPA EEI and additional proposal requirements.

    The transition and commercialization strategy should include the following elements:

    a. A summary of transition and commercialization activities conducted during Phase I, and the Technology Readiness Level (TRL) achieved. Discuss the market, competitive landscape, potential stakeholders and end-users, and how the preliminary transition and commercialization path or paths may evolve during the Phase II project. Describe key proposed technical milestones during Phase II that will advance the technology towards product such as: prototype development, laboratory and systems testing, integration, testing in operational environment, and demonstrations.
    b. Problem or Need Statement. Briefly describe what you know of the problem, need, or requirement, and its significance relevant to a Department of Defense application and/or a private sector application that the SBIR/STTR project results would address. Is there a broader societal need you are trying to address? Please describe.
    c. Description of Product(s) and/or System Application(s). Identify the commercial product(s) and/or DoD system(s), or system(s) under development, or potential new

system(s). Identify the potential DoD end- users, Federal customers, and/or private sector customers who would likely use the technology.

d. Business Model(s)/Procurement Mechanism(s). Discuss your current business model hypothesis for bringing the technology to market. Describe plans to license, partner, or self-produce your product. How do you plan to generate revenue? Describe the resources you expect will be needed to implement your business models. Discuss your plan and expected timeline to secure these resources. Understanding DARPA's goal of creating and sustaining a U.S. military advantage, describe how you intend to develop your product and supply chains to enable this differentiation.
e. Target Market. Describe the market and addressable market for the innovation. Describe the customer sets you propose to target, their size, their growth rate, and the key reasons they would consider procuring the technology. Discuss the business economics and market drivers in the target industry. Describe competing technologies existent today on the market as well as those being developed in the lab. How has the market opportunity been validated? Describe the competition. How do you expect the competitive landscape may change by the time your product/service enters the market?
f. Funding Requirements. Describe your company's funding history. How much external financing have you raised? Describe your plans for future funding sources (internal, loan, angel, venture capital, etc.).
g. Transition and Commercialization Risks. Describe the major technology, market and team risks associated with achieving successful transition of the DARPA funded technology. DARPA is not afraid to take risks but we want to ensure that our awardees clearly understand the risks in front of them. What are the key risks in bringing your innovation to market? What are actions you plan to undertake to mitigate these risks?
h. Expertise/Qualifications of Team/Company Readiness. Describe the expertise and qualifications of your management, marketing/business development and technical team that will support the transition of the technology from the prototype to the commercial market and into government operational environments. Has this team previously taken similar products/services to market? If the present team does not have this needed expertise, how do you intend to obtain it? What is the financial history and health of your company (e.g., availability of cash, profitability, revenue growth, etc.)?
i. Anticipated Transition and Commercialization Results. Include a schedule showing the anticipated quantitative transition and commercialization results from the Phase II project at one year after the start of Phase II, at the completion of Phase II, and after the completion of Phase II (i.e., amount of additional investment, sales revenue, etc.). After Phase II award, the company is required to report actual sales and investment data in its Company Commercialization Report at least annually.

Advocacy Letters (OPTIONAL)* Feedback received from potential Commercial and/or DoD customers and other end-users regarding their interest in the technology to support their capability gaps. Advocacy letters that are faxed or e-mailed separately will NOT be accepted.

Letters of Intent/Commitment (OPTIONAL)* Relationships established, feedback received, support and commitment for the technology with one or more of the following: Commercial customer, DoD PM/PEO, a Defense Prime, or vendor/supplier to the Primes and/or other vendors/suppliers identified as having a potential role in the integration of the technology into fielded systems/products or those under development. Letters of Intent/Commitment that are faxed or e- mailed separately will NOT be accepted.

*Advocacy Letters and Letters of Intent/Commitment are optional, and should ONLY be submitted to substantiate any transition or commercialization claims made in the commercialization strategy. Please

DO NOT submit these letters just for the sake of including them in your proposal. These letters DO NOT count against any page limit.

In accordance with section 3-209 of DOD 5500.7-R, Joint Ethics Regulation, letters from government personnel will NOT be considered during the evaluation process.

d. Format of Cost Volume (Volume 3)

Proposers are required to use the Direct to Phase II – Volume 3: Cost Proposal Template (Excel Spreadsheet) provided under SBIR/STTR BAA FORMS & TEMPLATES at https://www.darpa.mil/work-with-us/for-small-businesses/participate-sbir-sttr-program. The Cost Volume (and supporting documentation) DOES NOT count toward the page limit of the Technical Volume.

e. Content of the Cost Volume (Volume 3)

Some items in the Cost Breakdown Guidance below may not apply to the proposed project. If such is the case, there is no need to provide information on each and every item.

ALL proposed costs should be accompanied by documentation to substantiate how the cost was derived. For example, if you proposed travel cost to attend a project-related meeting or conference, and used a travel website to compare flight costs, include a screen shot of the comparison. Similarly, if you proposed to purchase materials or equipment, and used the internet to search for the best source, include your market research for those items. You do not necessarily have to propose the cheapest item or supplier, but you should explain your decision to choose one item or supplier over another. It's important to provide enough information to allow contracting personnel to understand how the proposer plans to use the requested funds. If selected for award, failure to include the documentation with your proposal will delay contract negotiation, and the proposer will be asked to submit the necessary documentation to the Contracting Officer to substantiate costs (e.g., cost estimates for equipment, materials, and consultants or subcontractors). It is important to respond as quickly as possible to the Contracting Officer's request for documentation.

Cost Breakdown Guidance:

1. List all key personnel by name as well as by number of hours dedicated to the project as direct labor. Special tooling and test equipment and material cost may be included. The inclusion of equipment and material will be carefully reviewed relative to need and appropriateness for the work proposed. The purchase of special tooling and test equipment must, in the opinion of the Contracting Officer, be advantageous to the Government and should be related directly to the specific topic. These may include such items as innovative instrumentation and/or automatic test equipment. Title to property furnished by the Government or acquired with Government funds will be vested with DARPA; unless it is determined that transfer of title to the contractor would be more cost effective than recovery of the equipment by the DARPA.
2. Cost for travel funds must be justified and related to the needs of the project.
3. Cost sharing is permitted for proposals under this announcement; however, cost sharing is not required nor will it be an evaluation factor in the consideration of a proposal.
4. All subcontractor costs and consultant costs must be detailed at the same level as prime contractor costs in regard to labor, travel, equipment, etc. Provide detailed substantiation of subcontractor costs in your cost proposal. Enter this information in the Explanatory Material section of the on-line cost proposal form. The Supporting Documents Volume (Volume 5) may be used if additional space is needed.

For more information about cost proposals and accounting standards, see the DCAA publication titled "Audit Process Overview – Information for Contractors" available at: http://www.dcaa.mil.

f. Company Commercialization Report (Volume 4)

The Company Commercialization Report (CCR) allows companies to report funding outcomes resulting from prior SBIR and STTR awards. The Company Commercialization Report (CCR) is required for Phase I and Direct to Phase II proposals. Please refer to the DoD STTR Program BAA for full details on this requirement. Information contained in the CCR will not be considered by DARPA during proposal evaluations.

g. Supporting Documents (Volume 5)

In addition to required DoD documentation and certifications, small businesses may also submit additional documentation to support the Technical Volume (Volume 2) and the Cost Volume (Volume 3) in Volume 5. See Appendix A Introduction for **required** certifications that must be included in Volume 5. For additional information, see the SBIR 23.4 Annual Program Broad Agency Announcement (BAA) at https://www.defensesbirsttr.mil/SBIR-STTR/Opportunities/.

h. Fraud Waste and Abuse (Volume 6)

The Fraud, Waste and Abuse (FWA) training is required for Phase I and Direct to Phase II proposals. FWA training provides information on what represents FWA in the SBIR/STTR program, the most common mistakes that lead to FWA, as well as the penalties and ways to prevent FWA in your firm. This training material must be thoroughly reviewed once per year. Plan ahead and leave ample time to complete this training based on the proposal submission deadline. Knowingly and willfully making any false, fictitious, or fraudulent statements or representations may be a felony under the Federal Criminal False Statement Act (18 U.S.C. Sec 1001), punishable by a fine of up to $10,000, up to five years in prison, or both. Understanding the indicators and types of fraud, waste, and abuse that can occur is critical for the SBIR/STTR awardees' role in preventing the loss of research dollars.

AMENDMENT 1

DARPA SBIR 23.4 Topic Index
Release 5

HR0011SB20234-08	2D Polyglots
HR0011SB20234-09	Passive Analytics for Remote Quantification of External Resources (PARQER)
HR0011SB20234-10	Assessing Virtual Private Network (VPN) Networthiness (AVN)
HR0011SB20234-11	Electronic Control Unit Authentication in Autonomous Vehicles (ECU2A)
HR0011SB20234-12	Network Black Box (NBB)
HR0011SB20234-13	5G Test Environment (5GTE)

AMENDMENT 1

HR0011SB20234-08 TITLE: 2D Polyglots

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Advanced computing and software

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 polyglots (dual embedded formats) for existing 2-dimensional codes (e.g., QR codes) that enable high-bandwidth, secure data transfer. Assess potential security vulnerabilities in polyglot approaches.

DESCRIPTION: DoD employees are interacting with physical-cyber data transfers at an ever-increasing rate; simply walking through an airport might require scanning 2-dimensional (2D) codes numerous times to receive basic goods and services, such as food menus and flight boarding passes. One of the most prevalent types of 2D codes is Quick Response (QR) code originating in 1994 from a Japanese automotive company. With the widespread adoption of mobile phones, QR codes have become a standard to store and transfer data in a physical format. The convenience that QR codes provide comes with certain limitations, such as the amount of data it can store and a balance between usability and security. 2D codes (e.g., QR codes, Data Matrix, MaxiCode, PDF417) are designed and optimized for a specific task; for example, data matrix codes used by shipping are fast to scan, however they only store 1.55kb of data as compared to 3kb for QR v4. 2D codes are often represented pictographically as part of printed media, such as a menu in a restaurant. They have low data density as a result of error correction and robustness to environmental effects (e.g., scratches). To increase the data density, preserve the inherent optimizations of each format, and ensure backwards compatibility, this study will investigate combining formats into 2D polyglots. In this context, a polyglot is a format that is valid in multiple computer programs. Polyglots are possible by combining two or more formats, each of which are able to be interpreted by multiple programs as having a valid format, for example, a file which is both a picture and a PowerPoint presentation.

This study will investigate the effects that 2D polyglots have in QR codes and their potential to reduce the attack surface and increase data density. A basis of confidence that polyglots can exist in 2D codes is the known, trivial case of a 2D code imbedded in another 2D code [D14]. For more than a decade it has been widely known that current 2D codes have inherent vulnerabilities [D15, F19, K10]. Usability was heavily favored over security in the design of these codes. This imbalance led to a widely adopted standard with pervasive vulnerabilities. Attacks can take advantage of error correction algorithms and data sparsity to exploit 2D formatting assumptions and the inconsistences which software makes when interpreting a 2D code. For example, standard QR codes have orientation markers and data is only parsed in one direction; polyglot QR codes can contain multiple, non-conflicting formats that can be read independently based on approach direction.Finally, to ensure current systems and software can still be used, any enhancements to the SOTA must also be backwards compatible. Introducing new software and standards would inevitably have new and possibly unintended effects on security and efficiency.

PHASE I: This topic is soliciting Direct to Phase II (DP2) proposals only. Proposers interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific and technical

merit and feasibility described above have been met and describe the potential commercial applications. DP2 documentation should include:

- Technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD insertion opportunity, and risks/mitigations, and assessments;
- Presentation materials and/or white papers;
- Technical papers;
- Test and measurement data;
- Prototype designs/models;
- Performance projections, goals, or results in different use cases; and,
- Documentation of related topics such as how the proposed SUP solution can enable more realistic cyber training.

This collection of material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and ability in networking, computer science, mathematics, and software engineering. For detailed information on DP2 requirements and eligibility, please refer to the DoD BAA and the DARPA Instructions for this topic.

PHASE II: The goal of 2D Polyglots is to develop a QR code that can hold more data while maintaining backwards compatibility and to identify vulnerabilities present in current 2D codes.DP2 proposals should propose a research design to achieve the following goals:

- Develop a protype system to demonstrate feasibility for producing 2D polyglots in a platform independent language (e.g., python 3.0, Golang);
- Identify vulnerabilities and possible mitigations in 2D and 2D polyglot codes;
- Detail a test plan, complete with proposed metrics and scope, for verification and validation of the system performance.

Phase II will culminate in a system demonstration using one or more compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program. The below schedule of milestones and deliverables is provided to establish expectations and desired results/end products for the Phase II effort.

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) (in person or virtual, as needed) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation.
- Months 3, 4, 5: Quarterly technical progress reports detailing technical progress made, tasks accomplished, major risks/mitigations, a technical plan for the remainder of Phase II (while this will normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 6: Interim technical progress briefing (with annotated slides) to the DARPA PM (in-person or virtual as needed) detailing progress made (include quantitative assessment of capability developed to date), tasks accomplished, major risks/mitigations, planned activities, and technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 7, 8, 9: Quarterly technical progress reports detailing technical progress made, tasks accomplished, major risks/mitigations, a technical plan for the remainder of Phase II (with necessary updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.

- Month 10/Final Phase II Deliverables: Final architecture with documented details, demonstrating diagnosing a malicious activity and unauthorized modification on software/hardware; documented application programming interfaces; any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the end of phase commercialization plan).

PHASE III DUAL USE APPLICATIONS: The Phase III work will be oriented towards transition and commercialization of the developed 2-D Polyglots technologies. The proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype software into a viable product or non-R&D service for sale in military or private sector markets. Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. Outcomes have the potential to significantly benefit the DoD and numerous commercial entities by improving knowledge of 2D codes including capabilities and vulnerabilities. Specifically, in the DoD space, 2D Polyglots technologies will be able to provide new data transfer methods utilizing 2D codes and highlight any potential vulnerabilities in current 2D codes used across the DoD enterprise. The development of polyglot technologies will have security benefits across the defense industrial base (DIB).

REFERENCES:

1. Dabrowski, A., Krombholz, K., Ullrich, J. and Weippl, E.R., 2014, November. QR inception: Barcode-in-barcode attacks. In Proceedings of the 4th ACM workshop on security and privacy in smartphones & mobile devices (pp. 3-10).
2. Dabrowski, A., Echizen, I. and Weippl, E.R., 2015, May. Error-correcting codes as source for decoding ambiguity. In 2015 IEEE Security and Privacy Workshops (pp. 99-105). IEEE.
3. Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., Schrittwieser, S., Sinha, M. and Weippl, E., 2010, November. QR code security. In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (pp. 430-435).
4. Focardi, R., Luccio, F.L. and Wahsheh, H.A., 2019. Usable security for QR code. Journal of Information Security and Applications, 48, p.102369.

KEYWORDS: Information assurance, computing and software technology, electro-optical sensors, cybersecurity, authentication, confidentiality, QR codes, Data Matrix, PDF417, MaxiCode, and 2D codes.

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil

AMENDMENT 1

HR0011SB20234-09 TITLE: Passive Analytics for Remote Quantification of External Resources (PARQER)

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Integrated Sensing and Cyber, Advanced computing and Software

OBJECTIVE: The Passive Analytics for Remote Quantification of External Resources (PARQER) SBIR topic seeks to develop and demonstrate novel techniques to passively assess the security posture of remote networks/subnetworks, without requiring any special network accesses.

DESCRIPTION: The near-constant stream of news reports on the compromise of systems and networks across government and commercial sectors reveals the challenges of securing large networks of systems with complicated topologies [1] [2] [3] [4]. The inherent asymmetry of effort required to defend an asset vs. effort to gain illicit access to an asset favors attackers that can spend as much time as necessary to locate vulnerable targets (e.g., a server that administrators neglected to patch [5], or a network configured with overly permissive firewall policies [6]). In such an environment where the attacker is advantaged, network administrators and security officers practice defense in depth [7] [8] by reducing the network attack surface and deploying an array of security mechanisms and technologies such as firewalls and intrusion detection/ prevention systems. The extent of an organization's efforts to minimize network attack surfaces and deploy defensive mechanisms can be largely unknown (e.g., due to poor documentation), even to the organization itself [9]. Often and unfortunately, details about the deployed security mechanisms (or the lack thereof) are only made available after an organization's network is compromised, and when forensic analysts conduct a postmortem of the attack [10] [11]. For the Department of Defense (DoD) and Intelligence Community (IC), the same problem exists and is compounded by the distinction between, and respective operational responsibilities of, network owners/operators and defenders such as Cybersecurity Service Provider (CSSPs) and Cyber Protection Teams (CPTs). Within the DoD/IC, CPTs are tasked with defending critical military networks; whereas CSSPs are responsible for the continuous monitoring and vulnerability patching of networks, and conducting threat-oriented missions to defeat cyber adversaries. [12] Similar to commercial organizations, critical details of network topology, configuration [13], and security posture [14] are often poorly documented and not immediately available to external responders (such as CPTs). An additional complicating factor of having network knowledge spread among different organizations and individuals (CPTs and CSSPs) is that it makes it difficult to have an accurate holistic picture of the security posture of lower-tier networks at any given time. It is therefore of critical importance for the DoD/IC and large commercial network owners to be able to quickly and passively assess the defensive posture of a remote network/subnetwork in a way that does not require any special access to the network.

PHASE I: The PARQER SBIR topic is soliciting Direct to Phase II (DP2) proposals only, which must include supporting documentation of Phase 1 feasibility. Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype system; definition and characterization of system properties/technology capabilities desirable for DoD/IC/Government and civilian/commercial use; and capability/performance comparisons with existing state-of-the-art technologies/methodologies (competing approaches). Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and also describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD/IC insertion opportunity, risks/mitigations, and technology assessments;
- presentation materials and/or white papers;
- technical papers;

- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases; and,
- documentation of related topics such as how the proposed PARQER solution can enable passive, remote assessment of network/subnetwork security posture.

The collection of Phase I feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of software engineering, data analytics, network security, and cybersecurity. For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

PHASE II: The PARQER DP2 SBIR topic seeks to develop and demonstrate novel techniques to enable passive assessment of the security posture of remote networks/subnetworks, without requiring any special access to the network. Most current tools and techniques employed by security operations centers are based on active interrogation. The tools and techniques are often too noisy (e.g., high volumes of alerts and high false positive rates), do not generalize across security mechanisms (i.e., the tools are siloed), and have significant blind spots (e.g., false negatives). Ideal PARQER solutions would overcome such limitations of active techniques, as well as be resistant to intentional misdirection and evasion. PARQER solutions must have the ability to provably scale yet provide fine resolution of the analyzed network. Successful PARQER proposals should clearly describe how proposed combinations of data and analytic techniques will provide high accuracy results in a landscape of ever-evolving security products.Phase II will culminate in a prototype system demonstration using one or more compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program (e.g., Signature Management using Operational Knowledge and Environments (SMOKE), which seeks to develop data-driven tools to automate the planning and execution of threat-emulated cyber infrastructure needed for network security assessments). The Phase II Option period will further mature the technology for insertion into a DoD/Intelligence Community (IC) Acquisition Program, another Federal agency; or commercialization into the private sector. The below schedule of milestones and deliverables is provided to establish expectations and desired results/end products for the Phase II and Phase II Option period efforts.

Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in the proposal, including the below:

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation;
- Months 4, 7, 10: Quarterly technical progress reports detailing technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM;
- Month 12: Interim technical progress briefing (with annotated slides) to the DARPA PM detailing progress made (including quantitative assessment of capabilities developed to date), tasks accomplished, risks/mitigations, planned activities, technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM;
- Months 15, 18, 21: Quarterly technical progress reports detailing technical progress made, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (with necessary

updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM;

- Month 24: Final technical progress briefing (with annotated slides) to the DARPA PM. Final architecture with documented details; a demonstration of the passive assessment of the security posture of remote networks/subnetworks; documented APIs; and any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the commercialization plan);
- Month 30 (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization; and,
- Month 36 (Phase II Option period): Final Phase II Option period demonstration and technical progress briefing (with annotated slides) to the DARPA PM including prototype performance against existing state-of-the-art technologies, including quantitative metrics of system performance.

PHASE III DUAL USE APPLICATIONS: Phase III Dual use applications (Commercial DoD/Military): PARQER has potential applicability across DoD/IC/Government and commercial entities. For DoD/IC/Government, PARQER is extremely well-suited to address one of the biggest issues in government information security today by providing the ability to quickly and passively assess the defensive posture of a remote network/subnetwork. PARQER has the same applicability for the commercial sector. Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. The Phase III work will be oriented towards transition and commercialization of the developed PARQER technologies. For Phase III, the proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype into a viable product or non-R&D service for sale in government or private sector markets. Primary PARQER support will be to national efforts to help secure government and commercial networks. Results of PARQER are intended to improve the ability of network owners across government and industry to quickly find the root causes of network compromise incidents, and rapidly mitigate the situation, ultimately improving the security posture of their networks.

REFERENCES:

1. PortSwigger. 2022. The Daily Swig, Cybersecurity News and Views. https://portswigger.net/daily-swig/data-breach
2. SecureLink. 2022. Recent Data Breaches in the News. https://www.securelink.com/resources/data-breach-news/
3. Cybersecurity Ventures. 2022. Today's Top Cybersecurity News Stories. https://cybersecurityventures.com/cybercrime-news/
4. The New York times. "How a Cyberattack Plunged a Long Island County Into the 1990s." 2022. https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html
5. Robb, Drew. "Is Neglect Driving the Surge in Cybersecurity Breaches?" 2022. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/neglect-driving-surge-cybersecurity-breaches.aspx
6. Fugue. "A Technical Analysis of the Capital One Cloud Misconfiguration Breach." 2019. https://www.fugue.co/blog/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach
7. The Department of Homeland Security's National Cybersecurity and Communications Integration Center and Industrial Control Systems Cyber Emergency Response Team. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. 2016. (Available at

https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)

8. National Security Agency. Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. 2010. (Available at https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf)
9. Burton, Dave. "The Dangers of Firewall Misconfigurations and How to Avoid Them." 2020. https://www.akamai.com/blog/security/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them
10. Gartner. "Is the Cloud Secure?" 2019. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure
11. Whittaker, Zack. "Equifax breach was 'entirely preventable' had it used basic security measures, says House report." 2018. https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/
12. Joint Publication 3-12. Cyberspace Operations. 2018. Available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
13. Marius Musch, Robin Kirchner, Max Boll, and Martin Johns. 2022. Server-Side Browsers: Exploring the Web's Hidden Attack Surface. In Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '22). Association for Computing Machinery, New York, NY, USA, 1168–1181. https://doi.org/10.1145/3488932.3517414. Available at https://loxo.ias.cs.tu-bs.de/papers/2022_AsiaCCS_SSBrowsers.pdf
14. Bo Lu, Xiaokuan Zhang, Ziman Ling, Yinqian Zhang, and Zhiqiang Lin. 2018. A Measurement Study of Authentication Rate-Limiting Mechanisms of Modern Websites. In Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC '18). Association for Computing Machinery, New York, NY, USA, 89–100. https://doi.org/10.1145/3274694.3274714. Available at https://yinqian.org/papers/acsac18a.pdf

KEYWORDS: network security, cybersecurity, defense in depth, passive network analytics

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil

AMENDMENT 1

HR0011SB20234-10 TITLE: Assessing Virtual Private Network (VPN) Networthiness (AVN)

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Integrated Sensing and Cyber, Advanced computing and Software

OBJECTIVE: The Assessing Virtual Private Network (VPN) Networthiness (AVN) SBIR topic seeks to develop and demonstrate techniques and systems for automatically analyzing third-party commercial VPN solutions to determine the actual operational privacy profile/performance of such services.

DESCRIPTION: Following the COVID-19 pandemic, and the concomitant increase in remote work, organizations and teleworkers sought solutions to keep their connections private and their workplace communications confidential. In other scenarios around the world, populations have sought private and secure solutions to circumvent restrictions on internet access placed on them by authoritarian regimes. It is therefore unsurprising that commercial VPN services have experienced substantial increases in demand over recent years [1, 2, 3]. The surge in VPN service demand has caused an increase in supply to the extent that (for example) the Google Play Store houses several hundred different apps that offer free (for examples, see [4]) and paid VPN services advertising increased privacy, high-speed bandwidth, large numbers of egress servers, access to censored websites, etc. [5] Even though users may be able to easily differentiate between fast and slow VPN services by merely using the service, unfortunately there are no outward signs they can use to quantify the privacy provided by VPN services. As such, users who employ such services to increase their privacy, may in fact be revealing their data to remote networks of less trustworthiness than their own local networks [6, 7]. It is therefore important to be able to proactively and continuously evaluate the properties and quality of protection that a commercial VPN solution offers. With rare exception [8], existing reviews of VPN services are typically conducted by technology journalists and are therefore limited to assessments of the VPN performance (e.g., speed), price, user friendliness (e.g., ease-of-use), features and supported protocols (e.g., see [9]).The AVN SBIR topic seeks to address this shortfall by developing and demonstrating techniques and systems for automatically analyzing third-party commercial VPN solutions to determine their networthiness, where networthiness considerations align with those of the Department of Defense (DoD) and Intelligence Community (IC) [10].

PHASE I: The AVN SBIR topic is soliciting Direct to Phase 2 (DP2) proposals only, which must include supporting documentation of Phase I feasibility. Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype system; definition and characterization of system properties/technology capabilities desirable for DoD/IC/government and civilian/commercial use; and capability/performance comparisons with existing state-of-the-art technologies/methodologies (competing approaches). Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and also describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD/IC insertion opportunity, risks/mitigations, and technology assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases; and,
- documentation of related topics such as how the proposed AVN solution can enable accurate and reliable analysis of third- party VPN solutions.

The collection of Phase 1 feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of software engineering, network security, privacy, analytics, and machine learning. For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

PHASE II: The AVN DP2 SBIR topic seeks to develop and demonstrate techniques and systems for automatically analyzing third-party commercial VPN solutions to determine the actual operational privacy profile/performance of such services. AVN solutions will provide an objective quantification of the privacy-related performance of third-party VPN services across platforms (e.g., Android, iPhone, PC, MAC, Ubuntu, etc.). Ideal solutions would require limited manual intervention and not rely on information elicited by the VPN service provider. AVN approaches will need to provably scale with the large number of available and future commercial VPN services. Ideally, AVN solutions would enable a user to tailor analyses to specific requirements as VPNs offer varying privacy protections that are not uniformly valuable to every user. DP2 proposals should:

- describe a proposed framework design/architecture to achieve the above stated goals;
- present a plan for maturation of the framework to a demonstrable prototype system; and
- detail a test plan, complete with proposed quantitative metrics for privacy, and for verification and validation of the prototype system performance.

Phase II will culminate in a prototype system demonstration using one or more compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program, for example, the Signature Management using Operational Knowledge and Environments (SMOKE) [11] program, which seeks to develop data-driven tools to automate the planning and execution of threat-emulated cyber infrastructure needed for network security assessments.

The Phase II Option period will further mature the technology for insertion into a DoD/ IC Acquisition Program, another Federal agency, or commercialization into the private sector.

The below schedule of milestones and deliverables is provided to establish expectations and desired results/end products for the Phase II and Phase II Option period efforts.

Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in the proposal, including the below:

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation.
- Months 4, 7, 10: Quarterly technical progress reports detailing technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 12: Interim technical progress briefing (with annotated slides) to the DARPA PM detailing progress made (including quantitative assessment of capabilities developed to date), tasks accomplished, risks/mitigations, planned activities, technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.

- Month 15, 18, 21: Quarterly technical progress reports detailing technical progress made, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (with necessary updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 24: Final technical progress briefing (with annotated slides) to the DARPA PM. Final architecture with documented details; a demonstration of the ability to automatically analyze third-party commercial VPN solutions; documented application programming interfaces; and any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the commercialization plan).
- Month 30 (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization.
- Month 36 (Phase II Option period): Final Phase II Option period technical progress briefing (with annotated slides) to the DARPA PM including prototype performance against existing state-of-the-art technologies, including quantitative metrics for assessment of privacy features/capabilities.

PHASE III DUAL USE APPLICATIONS: AVN has potential applicability across DoD/IC/government and commercial entities. For DoD/IC/government, AVN is extremely well-suited for proactive and continuous assessment of privacy features/performance of various VPN services. AVN has the same applicability for the commercial sector and has the potential to provide individuals worldwide with reliable private connections and communications. Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. The Phase III work will be oriented towards transition and commercialization of the developed AVN technologies. For Phase III, the proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype into a viable product or non-R&D service for sale in government or private sector markets. Primary AVN support will be to national efforts to help secure government, commercial, and personal networks and devices against advanced persistent threats that target vulnerable VPN devices. Results of AVN are intended to improve understanding of the risks associated with VPNs, across government and industry.

REFERENCES:

1. "The Impact of COVID-19 on VPN Usage and Streaming Habits", https://www.cartesian.com/the-impact-of-covid-19-on-vpn-usage-and-streaming-habits/
2. "VPN Demand Surges Around the World", https://www.top10vpn.com/research/vpn-demand-statistics/
3. "Four Risks to Consider with Expanded VPN Deployments", https://www.f5.com/labs/articles/cisotociso/four-risks-to-consider-with-expanded-vpn-deployments
4. "Free VPN Ownership & Security Investigations Update", https://www.top10vpn.com/research/free-vpn-investigations/ownership-risk-index-update/
5. Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In Proceedings of the 2016 Internet Measurement Conference (IMC '16). Association for Computing Machinery, New York, NY, USA, 349–364. https://doi.org/10.1145/2987443.2987471. Available at https://www.cs.umd.edu/class/spring2017/cmsc818O/papers/vpn-app-risks.pdf
6. O. Akgul, R. Roberts, M. Namara, D. Levin and M. L. Mazurek, "Investigating Influencer VPN Ads on YouTube," 2022 IEEE Symposium on Security and Privacy (SP), 2022, pp. 876-892, doi:

10.1109/SP46214.2022.9833633. Available at https://www.cs.umd.edu/~akgul/papers/vpn-ads.pdf
7. Free VPNs are bad for your privacy", https://techcrunch.com/2020/09/24/free-vpn-bad-for-privacy/
8. Grauer, Yael. "Security and Privacy of VPNs Running on Windows 10." Consumer Reports Digital Lab. 2021. Available at https://digital-lab-wp.consumerreports.org/wp-content/uploads/2021/12/VPN-White-Paper.pdf
9. https://www.top10vpn.com/reviews/
10. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2791320/nsa-cisa-release-guidance-on-selecting-and-hardening-remote-access-vpns/
11. Defense Advanced Research Projects Agency, SMOKE Broad Agency Announcement HR001122S0006 (2021) (Available at https://sam.gov/opp/6ab1fdaedfd6411ba966025cd74e467c/view)

KEYWORDS: custom analytics, network security, privacy, virtual private network

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil

AMENDMENT 1

HR0011SB20234-11 TITLE: Electronic Control Unit Authentication in Autonomous Vehicles (ECU2A)

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): FutureG, Trusted AI and Autonomy, Advanced Computing and Software, Integrated Sensing and Cyber

OBJECTIVE: The objective of the Electronic Control Unit Authentication in Autonomous Vehicles (ECU2A) Direct to Phase 2 (DP2) SBIR topic is to develop prototype systems to authenticate, monitor, and detect malicious activities in Electronic Control Units (ECUs) of modern intelligent military and civilian vehicles.

DESCRIPTION: ECUs are one of the most critical embedded systems that control many subsystems in a vehicle [1]. A vehicle's distributed network of ECUs is responsible for the control/functionality of the engine and transmission system, as well as for the control/functionality of the vehicle's comfort and entertainment systems. Due to the extensive and growing use of ECUs in modern vehicles, and the associated increased costs and complexities they bring (e.g., due to multiple manufacturers, system integration requirements) [2], many vehicle manufacturers have adapted their manufacturing models and design flows to use the intellectual property of third-party ECU manufacturers, and outsource the fabrication of ECU hardware to offshore foundries to reduce the cost and time-to-market for their vehicles. Unfortunately, outsourcing ECU fabrication raises important security concerns [3, 4] for intelligent vehicles used by the civilian sector as well as US expeditionary forces abroad.The various Internet-of-Things (IoT) networks (e.g., Cellular, Local and Personal Area Networks, Low Power Wide Area Networks, and Mesh networks [5]) and the continuing increases in the scale of networked systems offers unprecedented interconnectivity of electronic devices, to include ECUs. Because of the ubiquitous nature and large attack surfaces of IoT networks, threats such as man-in-the-middle attacks, denial of service attacks, and hijacking of services attacks [6] can be successfully executed through bypassing the authentication process of ECUs. The consequences of such attacks can increase in severity if the ECUs are tampered with during production [7, 8, 9], prior to installation in the vehicle. Therefore, it is critical to have the ability to securely authenticate vehicular ECUs and to continuously monitor them for detection of malicious activity.

PHASE I: The ECU2A SBIR topic is soliciting DP2 proposals only, which must include supporting documentation of Phase I feasibility. Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype system; definition and characterization of system properties/technology capabilities desirable for DoD/IC/government and civilian/commercial use; and capability/performance comparisons with existing state-of-the-art technologies/methodologies (competing approaches). Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and also describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD/IC insertion opportunity, risks/mitigations, and technology assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases; and,
- documentation of related topics such as how the proposed ECU2A solution can enable secure authentication and continuous monitoring of ECUs in modern intelligent vehicles.

The collection of Phase I feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of software engineering, network security, cyber security, analytics, and machine learning. For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

PHASE II: The objective of the ECU2A DP2 SBIR topic is to develop prototype systems to authenticate, monitor, and detect malicious activities in ECUs of modern intelligent military and civilian vehicles.ECU2A will develop new hardware/software/component verification methods, algorithms, and machine learning models to improve vehicular ECU security. Strong ECU2A proposals should address several technical challenges, such as:

- effective tools and algorithms for one-time ECU authentication and continuous ECU monitoring schemes;
- models capable of rapidly identifying compromised ECUs;.
- ECU software/hardware validation techniques, prior to and after installment;
- zero-overhead, non-intrusive monitoring schemes, that do not require direct ECU access, for easy and secure deployment;
- techniques to rapidly minimize the connection/communication between the source of malicious activity and a targeted ECU;
- capabilities to detect hardware/software trojans with no reverse-engineering techniques;
- monitoring methods for devices operating on a broad range of ECU components, and which have an air-gapped nature.

Phase II will culminate in a demonstration of the application and validation of ECU2A-developed technologies for detecting malicious activity against one or more concrete technological use cases of integrated software systems.Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in the proposal, including the below:

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation.
- Months 4, 7, 10: Quarterly technical progress reports detailing technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 12: Interim technical progress briefing (with annotated slides) to the DARPA PM detailing progress made (including quantitative assessment of capabilities developed to date), tasks accomplished, risks/mitigations, planned activities, technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 15, 18, 21: Quarterly technical progress reports detailing technical progress made, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (with necessary updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 24: Final technical progress briefing (with annotated slides) to the DARPA PM. Final architecture with documented details; a demonstration of the ability to authenticate, monitor, and

detect malicious activities in ECUs; documented application programming interfaces; and any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the commercialization plan).

- Month 30 (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization.
- Month 36 (Phase II Option period): Final Phase II Option period technical progress briefing (with annotated slides) to the DARPA PM including prototype performance against existing state-of-the-art technologies, including quantitative metrics for assessment of prototype features/capabilities.

PHASE III DUAL USE APPLICATIONS: ECU2A has potential applicability across DoD/IC/government and commercial entities. For DoD/IC/government, ECU2A is extremely well-suited for improving the security of intelligent vehicles used by US expeditionary forces abroad. ECU2A has the same applicability for the commercial sector.Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. The Phase III work will be oriented towards transition and commercialization of the developed ECU2A technologies. For Phase III, the proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype into a viable product or non-R&D service for sale in government or private sector markets. Primary ECU2A support will be to national efforts to help secure military and commercial intelligent vehicle ECUs against threats that target vulnerabilities. Results of ECU2A are intended to improve understanding of the threats and vulnerabilities associated with the increasing use of intelligent vehicles, across government and industry.

REFERENCES:

1. Jaks, L. (2014). Security Evaluation of the Electronic Control Unit Software Update Process. Available at: http://kth.diva-portal.org/smash/get/diva2:934083/FULLTEXT01.pdf
2. Electronics Sourcing. (2022). How Many Chips are in Our Cars?https://electronics-sourcing.com/2022/05/04/how-many-chips-are-in-our-cars
3. R. Kurachi et al., "Evaluation of Security Access Service in Automotive Diagnostic Communication," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1-7, doi: 10.1109/VTCSpring.2019.8746714. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8746714.
4. Spaan, R.. Secure updates in automotive systems. Nijmegen: Radboud University(2016): 1-71. Available at: https://www.ru.nl/publish/pages/769526/z_remy_spaan.pdf
5. IotaComm. 2020. Four Types Of IoT Wireless Networks. https://www.iotacommunications.com/blog/types-of-iot-networks/
6. Huq, N. et al. “Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and OtherConnected Technologies.” Trend Micro Research. 2021. Available at: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf
7. Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusiondetection." 25th USENIX Security Symposium (USENIX Security 16). 2016. Available at https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_cho.pdf
8. Kim, Kyounggon, et al. "Cybersecurity for autonomous vehicles: Review of attacks and defense."Computers & Security, Volume 103 (2021): 102150. ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102150.
9. Wasicek, A. and Weimerskirch, A. “Recognizing manipulated electronic control units,” . SAE Technical Paper 2015-01-0202, 2015, https://doi.org/10.4271/2015-01-0202.. Available at https://ptolemy.berkeley.edu/projects/chess/pubs/1111/autoids_v2_preprint1.pdf.

AMENDMENT 1

KEYWORDS: Electronic Control Units, Cyber Security, Intrusion Detection, Intelligent Vehicles

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil

AMENDMENT 1

HR0011SB20234-12 TITLE: Network Black Box (NBB)

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Integrated Sensing and Cyber, Advanced computing and Software

OBJECTIVE: The Network Black Box Direct to Phase 2 (DP2) SBIR topic seeks to develop and demonstrate a system prototype capable of automatically retaining, retrieving, and analyzing network data to support threat detection and response efforts by cyber security operations teams.

DESCRIPTION: Today's enterprise networks are challenged by a myriad of cyber threats that can jeopardize the confidentiality, integrity, and availability of a network. An organization's enterprise security controls aim to protect the organization's networks against threats from hackers, malicious software, and attempts to steal sensitive information [1]. Threat hunting and incident response tactics, techniques, and procedures (TTPs) employed by an organization's cyber security operations teams help protect the networks by continuously monitoring for threats in progress that evade security controls and breach the network [2]. Despite significant investment in enterprise security controls, and the collection and use of diverse and voluminous datasets for threat hunting and incident response, many organizations lack the infrastructure capacity and resources to store key enterprise network security data in a reliable, efficient, and cost-effective way, for durations comparable to the average dwell time [3] of cyber attackers (i.e., the amount of time an attacker spends on a target network before being detected). Dwell times, which vary based on region and other factors, can average up to two months, giving attackers plenty of time to wreak havoc on the target network [4]. In addition, shortfalls in infrastructure capacity and resources adversely impacts an organization's ability to efficiently and effectively conduct incident response forensics on the network security data, once intrusion is detected.Organizations across government and industry would benefit from a simple, yet powerful, reliable, efficient, and cost-effective mechanism to support automated retention, retrieval, and analysis of key enterprise network data for security operations teams to conduct incident response forensics, such as root cause analysis [5] and lateral movement [6] detection, ex post facto.

PHASE I: The Network Black Box SBIR topic is soliciting Direct to Phase 2 (DP2) proposals only, which must include supporting documentation of Phase 1 feasibility. Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype system; definition and characterization of system properties/technology capabilities desirable for DoD/IC/government and civilian/commercial use; and capability/performance comparisons with existing state-of-the-art technologies/methodologies (competing approaches). Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and also describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD/IC insertion opportunity, risks/mitigations, and technology assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases; and,
- documentation of related topics such as how the proposed Network Black Box solution can enable the retention, retrieval, and analysis of network data to support threat detection and response efforts by security operations teams.

The collection of Phase 1 feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of cyber operations, software engineering, network security, data analytics, artificial intelligence, and machine learning. For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

PHASE II: The Network Black Box DP2 SBIR topic seeks to develop and demonstrate a system prototype capable of automatically retaining, retrieving, and analyzing network data to support threat detection and response efforts by security operations teams. It is envisioned that Network Black Box approaches will take the form of a physical or virtual appliance with an intuitive user interface supporting at least the two use cases stated previously, namely root cause analysis and lateral movement detection. Proposed solutions should enable organizations to retain and analyze enterprise network data for at least one year for a network consisting of at least 10,000 hosts. Strong Network Black Box proposals will provide experimental evidence and a quantitative analysis on the cost, capacity, and scalability of such a capability, and present preliminary evidence on the usefulness of the retained data for root cause analysis, lateral movement detection, and any additional use cases.

DP2 proposals should:

- describe a proposed framework design/architecture to achieve the above stated goals;
- present a plan for maturation of the framework to a demonstrable prototype system; and
- detail a test plan, complete with proposed quantitative metrics for verification and validation of the prototype system performance.

Phase II will culminate in a prototype system demonstration using compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program (e.g., the Cyber Agents for Security Testing and Learning Environments (CASTLE) [7] program which seeks to generate data-driven, machine-readable descriptions of how attacker tools behave, how attack paths unfold, and how to label observable attack behavior; and the Signature Management using Operational Knowledge and Environments (SMOKE) [8] program which seeks to assist red teams with planning with deploying TTPs to evade network defenders in order to achieve assessment objectives (e.g., lateral movement in networks) and assess how networks perform against malicious cyber actors (MCAs)).

The Phase II Option period will further mature the technology for insertion into a DoD/ IC Acquisition Program, another Federal agency, or commercialization into the private sector.The below schedule of milestones and deliverables is provided to establish expectations and desired results/end products for the Phase II and Phase II Option period efforts.

Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in the proposal, including the below:

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation.
- Months 4, 7, 10: Quarterly technical progress reports detailing technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.

- Month 12: Interim technical progress briefing (with annotated slides) to the DARPA PM detailing progress made (including quantitative assessment of capabilities developed to date), tasks accomplished, risks/mitigations, planned activities, technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 15, 18, 21: Quarterly technical progress reports detailing technical progress made, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (with necessary updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 24: Final technical progress briefing (with annotated slides) to the DARPA PM. Final architecture with documented details; a demonstration of the ability to automatically retain, retrieve, and analyze network data to support threat detection and response efforts by security operations teams; documented application programming interfaces; and any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the commercialization plan).
- Month 30 (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization.
- Month 36 (Phase II Option period): Final Phase II Option period technical progress briefing (with annotated slides) to the DARPA PM including prototype performance against existing state-of-the-art technologies, including quantitative metrics for assessment of privacy features/capabilities.

PHASE III DUAL USE APPLICATIONS: Network Black Box has potential applicability across DoD/IC/government and commercial entities. For DoD/IC/government, Network Black Box is extremely well-suited for forensic analysts tasked with conducting postmortems after an organization's network is compromised. Network Black Box has the same applicability for the commercial sector. Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. The Phase III work will be oriented towards transition and commercialization of the developed Network Black Box technologies. For Phase III, the proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype into a viable product or non-R&D service for sale in government or private sector markets. Primary Network Black Box support will be to national efforts to help secure government and commercial networks against MCAs that target critical networks. Results of Network Black Box are intended to improve understanding of MCA threats and improve detection and response actions across government and industry.

REFERENCES:

1. NIST SP 800-53 Revision 5. 2020. "Security and Privacy Controls for Information Systems and Organizations." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
2. Waqas, Iam. PrivacyAffairs. 2022. .https://www.privacyaffairs.com/threat-hunting-vs-incident-response/ \
3. Armor Defense. 2021. "Dwell Time as a Critical Security Success Metric." https://cdn.armor.com/app/uploads/2020/04/Ebook-DwellTime.pdf
4. Nayyar, Saryu. "Why The Dwell Time Of Cyberattacks Has Not Changed." 2021. https://www.forbes.com/sites/forbestechcouncil/2021/05/03/why-the-dwell-time-of-cyberattacks-has-not-changed/?sh=1ddedc37457d
5. Gross, Natalie. CDW StateTech. 2021. "Incident Response: The Steps to a Root Cause Analysis for State Government."
6. Cybertalk.org. 2022. https://www.cybertalk.org/what-is-lateral-movement-computing/

7. DARPA I2O. 2022. Broad Agency Announcement, Cyber Agents for Security Testing and LearningEnvironments (CASTLE) HR001123S0002. Available at https://sam.gov/opp/5fa7645fdf464f70b5c67e24585926f7/view.
8. DARPA I2O. 2021. Broad Agency Announcement, Signature Management using Operational Knowledge and Environments (SMOKE) HR001122S0006. Available at https://sam.gov/opp/8832e2b8d9864169a234834eea89e5f1/view

KEYWORDS: Network Security, Cybersecurity, Incident Response, Threat Hunting, Artificial Intelligence, Machine Learning, Automation, Data Analytics

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil

AMENDMENT 1

R0011SB20234-13 TITLE: 5G Test Environment (5GTE)

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Integrated Sensing and Cyber, Advanced computing and Software

OBJECTIVE: The objective of the 5GTE Direct to Phase 2 (DP2) SBIR topic is to develop a scalable, open-source Internet of Things (IoT) fifth generation (5G) test environment capability to support research and development of nascent 5G technologies.

DESCRIPTION: 5GTE seeks to develop a 5G test environment for IoT devices to enable research, development, and experimentation with a broad range of 5G-capable devices, both static and mobile. The focus of 5GTE is to provide an open-source, realistic 5G radio access network to enable rapid prototyping of wireless protocols and applications including, but not limited to: cyber security, artificial intelligence, and edge-computing.

A key requirement of 5GTE is the ability to rapidly and accurately scale as new technologies and devices are introduced/become available. 5GTE must also provide remote access and device update capabilities. To broaden the range of supported devices and to facilitate development, 5GTE should have the ability to support different wireless communication technologies (e.g., fourth generation, wireless fidelity). 5GTE's network access should support high-fidelity quality of service for experimentation with different 3rd Generation Partnership (3GPP) [1] Project Release 17 [2] use cases.

While open-source 5G testbed architectures do exist [3], they do not fully support remote accessibility and management to allow for multiple experiments and tests to co-exist simultaneously.

PHASE I: The 5GTE SBIR topic is soliciting DP2 proposals only, which must include supporting documentation of Phase I feasibility. Phase I feasibility must be demonstrated through evidence of: a completed proof of concept/principal or basic prototype system; definition and characterization of system properties/technology capabilities desirable for DoD/IC/government and civilian/commercial use; and capability/performance comparisons with existing state-of-the-art technologies/methodologies (competing approaches).

Entities interested in submitting a DP2 proposal must provide documentation to substantiate that the scientific/technical merit and feasibility described above has been achieved and also describe the potential commercial applications. DP2 Phase I feasibility documentation should include, at a minimum:

- technical reports describing results and conclusions of existing work, particularly regarding the commercial opportunity or DoD/IC insertion opportunity, risks/mitigations, and technology assessments;
- presentation materials and/or white papers;
- technical papers;
- test and measurement data;
- prototype designs/models;
- performance projections, goals, or results in different use cases; and,
- documentation of related topics such as how the proposed 5GTE solution can enable research and development of nascent 5G technologies.

The collection of Phase I feasibility material will verify mastery of the required content for DP2 consideration. DP2 proposers must also demonstrate knowledge, skills, and abilities in the technical areas of: mobile communications, software engineering, network security, cyber security, programmable

networking, and artificial intelligence. For detailed information on DP2 requirements and eligibility, please refer to the DoD Broad Agency Announcement and the DARPA Instructions for this topic.

PHASE II: The objective of the 5GTE DP2 SBIR topic is to develop a scalable, open-source IoT 5G test environment capability to support research and development of nascent 5G technologies.
5GTE DP2 proposals should:

1. describe a proposed design/architecture to achieve the 5GTE goals, along with application programming interfaces that allow for an open IoT testbed infrastructure;
2. present a plan for maturation of the architecture to a prototype testbed to demonstrate accurate and scalable experimentation capabilities; and,
3. detail a test plan, complete with proposed metrics and scope (e.g., testbed structure, types/numbers of devices, etc.) for verification and validation of the testbed capabilities.

5GTE should have the ability to support multiple isolated environments to enable testing in parallel with security guarantees. Each isolated environment would support full standards compliant user authentication on the 5G core side, where the end devices can use programmable subscriber identity module cards; and the core would support network slicing capabilities.
Strong 5GTE proposals would include:

- additional scaling capabilities enabled via emulation of various end devices;
- solutions based on components with strong open-source development and community support, such as the technology projects that reside within the Linux Foundation [5]; and,
- a commercialization plan for the proposed 5GTE which articulates a clear vision for the potential business opportunities as 5G capabilities and standards evolve.

Phase II will culminate in a testbed demonstration using one or more compelling IoT use cases consistent with commercial opportunities and/or insertion into the DARPA/I2O Open, Programmable, Secure 5G (OPS-5G) program [4]. The below schedule of milestones and deliverables is provided to establish expectations and desired results/end product for the DP2 effort.

Schedule/Milestones/Deliverables: Proposers will execute the research and development (R&D) plan as described in the proposal, including the below:

- Month 1: Phase I Kickoff briefing (with annotated slides) to the DARPA Program Manager (PM) including: any updates to the proposed plan and technical approach, risks/mitigations, schedule (inclusive of dependencies) with planned capability milestones and deliverables, proposed metrics, and plan for prototype demonstration/validation.
- Months 4, 7, 10: Quarterly technical progress reports detailing technical progress to date, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (while this would normally report progress against the plan detailed in the proposal or presented at the Kickoff briefing, it is understood that scientific discoveries, competition, and regulatory changes may all have impacts on the planned work and DARPA must be made aware of any revisions that result), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 12: Interim technical progress briefing (with annotated slides) to the DARPA PM detailing progress made (including quantitative assessment of capabilities developed to date), tasks accomplished, risks/mitigations, planned activities, technical plan for the second half of Phase II, the demonstration/verification plan for the end of Phase II, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.
- Month 15, 18, 21: Quarterly technical progress reports detailing technical progress made, tasks accomplished, risks/mitigations, a technical plan for the remainder of Phase II (with necessary updates as in the parenthetical remark for Months 4, 7, and 10), planned activities, trip summaries, and any potential issues or problem areas that require the attention of the DARPA PM.

- Month 24: Final technical progress briefing (with annotated slides) to the DARPA PM. Final architecture with documented details; a demonstration of the ability to authenticate, monitor, and detect malicious activities in ECUs; documented application programming interfaces; and any other necessary documentation (including, at a minimum, user manuals and a detailed system design document; and the commercialization plan).
- Month 30 (Phase II Option period): Interim report of matured prototype performance against existing state-of-the-art technologies, documenting key technical gaps towards productization.
- Month 36 (Phase II Option period): Final Phase II Option period technical progress briefing (with annotated slides) to the DARPA PM including prototype performance against existing state-of-the-art technologies, including quantitative metrics for assessment of test environment features/capabilities.

PHASE III DUAL USE APPLICATIONS: 5GTE has potential applicability across DoD/IC/government and commercial entities. For DoD/IC/government, 5GTE is extremely well-suited for supporting research to investigate 5G capability enhancements and cyber risks. 5GTE has the same applicability for the commercial sector.

Phase III refers to work that derives from, extends, or completes an effort made under prior SBIR funding agreements, but is funded by sources other than the SBIR Program. The Phase III work will be oriented towards transition and commercialization of the developed 5GTE technologies. For Phase III, the proposer is required to obtain funding from either the private sector, a non-SBIR Government source, or both, to develop the prototype into a viable product or non-R&D service for sale in government or private sector markets.

Primary 5GTE support will be to national efforts to advance US 5G capabilities and to promote awareness of 5G risks to national security. Results of 5GTE are intended to enable accurate test and evaluation of nascent 5G technologies at scale, across government and industry.

REFERENCES:

1. 3GPP. 3GPP - A Global Initiative. https://www.3gpp.org/
2. 3GPP. 3GPP – The 5G Standard. https://www.3gpp.org/specifications-technologies/releases/release-17
3. Institute for the Wireless Internet of Things at Northeastern University. Testbeds to develop and experiment with open, programmable, 5G networks. https://open5g.info/testbeds/
4. DARPA Broad Agency Announcement: Open Programmable Secure 5G (OPS-5G), HR001120S0026, January 30, 2020. Available at https://beta.sam.gov/opp/6ee795ad86a044d1a64f441ef713a476/view
5. The Linux Foundation. The Linux Foundation. https://www.linuxfoundation.org/

KEYWORDS: Fifth Generation (5G), Internet of Things (IoT), Test Environment, Scalability, Open-source, Security, Cyber Security, Artificial Intelligence, and Edge-computing

TPOC-1: DARPA BAA Help Desk
Email: SBIR_BAA@darpa.mil