Broad Agency Announcement

Guaranteeing AI Robustness against Deception (GARD)

HR001119S0026

February 12, 2019

Defense Advanced Research Projects Agency
Information Innovation Office
675 North Randolph Street
Arlington, VA 22203-2114

Table of Contents

I. Funding Opportunity Description 5

A. Introduction 5

B. Program Description 6

C. Foundations 8

D. Multi-Modality 8

E. Program Structure 9

F. Technical Areas 9

G. Metrics 12

H. Evaluation Scenarios 14

I. Out of Scope 15

J. Schedule, Milestones, and Evaluation 15

K. Deliverables 18

II. Award Information 19

A. Awards 19

B. Fundamental Research 20

C. Disclosure of Information and Compliance with Safeguarding Covered Defense Information Controls 20

III. Eligibility Information 22

A. Eligible Applicants 22

B. Organizational Conflicts of Interest 23

C. Cost Sharing/Matching 24

D. Other Eligibility Requirements 24

IV. Application and Submission Information 25

A. Address to Request Application Package 25

B. Content and Form of Application Submission 25

C. Submission Dates and Times 37

D. Funding Restrictions 38

E. Other Submission Requirements 38

V. Application Review Information 42

A. Evaluation Criteria 42

B. Review and Selection Process 42

VI. Award Administration Information 44

A. Selection Notices 44

B. Administrative and National Policy Requirements....44
C. Reporting....47
VII. Agency Contacts....49
VIII. Other Information....50
A. Frequently Asked Questions (FAQs)....50
B. Proposers Day....50
C. Submission Checklist....50

PART I: OVERVIEW INFORMATION

- **Federal Agency Name:** Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)
- **Funding Opportunity Title:** Guaranteeing AI Robustness against Deception (GARD)
- **Announcement Type:** Initial Announcement
- **Funding Opportunity Number:** HR001119S0026
- **Catalog of Federal Domestic Assistance Numbers (CFDA):** 12.910 Research and Technology Development
- **Dates**
  - Posting Date: February 12, 2019
  - Proposers Day: February 6, 2019
  - Abstract Due Date: February 26, 2019, 12:00 noon (ET)
  - Proposal Due Date: April 11, 2019, 12:00 noon (ET)
  - BAA Closing Date: April 11, 2019, 12:00 noon (ET)
- **Anticipated Individual Awards:** DARPA anticipates multiple awards for Technical Area 1 and a single award for Technical Area 2.
- **Types of Instruments that May be Awarded:** Procurement contracts, cooperative agreements, grants or other transactions (OTs)
- **Agency Contacts**
  - **Technical POC**: Dr. Hava Siegelmann, Program Manager, DARPA/I2O
  - **BAA Email**: GARD@darpa.mil
  - **BAA Mailing Address**:

    DARPA/I2O
    ATTN: HR001119S0026
    675 North Randolph Street
    Arlington, VA 22203-2114
  - **I2O Solicitation Website:** http://www.darpa.mil/work-with-us/opportunities

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

DARPA is soliciting innovative research proposals in the area of theoretical foundations, principled algorithms, and evaluation frameworks that significantly improve the robustness of machine learning systems to adversarial attacks. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to current practices.

This Broad Agency Announcement (BAA) is being issued, and any resultant selection will be made, using procedures under Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016. Any negotiations and/or awards will use procedures under FAR 15.4 (or 32 CFR § 200.203 for grants and cooperative agreements). Proposals received as a result of this BAA shall be evaluated in accordance with evaluation criteria specified herein through a scientific review process.

DARPA BAAs are posted on the Federal Business Opportunities (FBO) website (https://www.fbo.gov/) and the Grants.gov website (https://www.grants.gov/).

The following information is for those wishing to respond to this BAA. *Proposers are strongly encouraged to read the entirety of this document, as information on interactions among technical areas (TAs) and information on evaluation, schedule, and deliverables is provided in sections other than those describing the particular TAs.*

A. Introduction

The GARD program will develop a new generation of defenses against deception attacks on machine learning (ML). The program is soliciting game-changing research proposals to develop theory, create defenses, and implement appropriate testbeds leading to robust, deception-resistant ML/AI algorithms. Proposed research should investigate defenses that address entire threat scenario classes. Specifically excluded is research solely focused on developing defenses to specific attacks rather than addressing broad issues of defensibility.

The growing sophistication and ubiquity of ML components in advanced systems dramatically increase capabilities, but as a byproduct, also increases the potential for new vulnerabilities. The current era of adversarial AI focuses on approaches where imperceptible perturbations to ML inputs could deceive an ML classifier, significantly altering its response. Such results have initiated a rapidly proliferating field of research characterized by ever more complex attacks that require progressively less knowledge about the ML system being attacked, while proving increasingly strong against defensive countermeasures.

The acceleration in ML attack capabilities has promoted an arms race. As defenses are developed to address new attack strategies and vulnerabilities, improved attack methodologies capable of bypassing the defense algorithms are created. The field now appears increasingly pessimistic, sensing that developing effective ML defenses may prove significantly more difficult than designing new attacks, leaving advanced systems vulnerable and exposed. Recent theoretical research also suggests the inevitability of adversarial attacks targeting the deep neural networks commonly used in advanced systems. In addition to developing strongly defensible AI algorithms, GARD seeks to ensure that advanced systems are robust to the perturbations encountered in real-world operation.

Although the field of Adversarial AI is relatively young, dozens of attacks and defenses have already been proposed. For instance, recent optimization-based adversarial training presents a promising defense based on a principled definition of robust ML that maintains classification accuracy in the presence of small, size-bounded perturbations added to the inputs. This approach is powerful since it is designed to work against any attack algorithm leading to those particular input perturbations. The resultant defense, however, has proved slow to train. More significantly, it is only capable of protecting against perturbing the inputs in a predetermined metric; deception attacks working in other metrics are still able to penetrate the defense.

At present, the Adversarial AI field lacks a comprehensive theoretical understanding of ML vulnerabilities. Failing to fully take into account ML's theoretical underpinnings leaves significant blind spots that can be exploited, and limits efforts to develop effective defenses. GARD seeks to establish theoretical ML system foundations to identify system vulnerabilities, characterize properties that will enhance system robustness and encourage the creation of effective defenses. Novel adversarial AI defenses may also gain insight and inspiration from biological systems (e.g., the immune system, interactions between bacteria and viruses, sensory perception), where multiple mechanisms work synergistically to increase robustness. Currently, ML defenses tend to be highly specific, and are effective only against particular attacks. GARD seeks to develop defenses with more generalized applicability capable of defending against broad categories of attack. Furthermore, current evaluation paradigms of AI robustness often focus on simplistic measures that are less relevant to security. To verify robustness and wide applicability, defenses generated under GARD will be measured in a novel testbed employing scenario-based evaluations.

In summary, GARD's purpose is to encourage both development of underlying theory and to functionally and substantially improve ML defensibility, leading to a new generation of defense approaches beyond current mathematical and algorithmic thinking.

B. Program Description

GARD has three objectives:

1. Create a sound theoretical foundation for defensible AI.
2. Develop principled, general defense algorithms.
3. Produce and apply a scenario-based evaluation framework to characterize which defense is most effective in a particular situation, given available resources. GARD defenses will be evaluated using realistic scenarios and large datasets.

C. Program Focus

GARD will focus on deception attacks that induce incorrect behavior in ML systems by manipulating their inputs. The program will develop defenses against attacks that have appeared to date in literature, as well as any attacks published during the program's four-year duration. GARD's defenses will consider many possible scenario factors, including:

1. Attacks at various learning phases: dataset poisoning in addition to inference time attacks that exploit extant system weaknesses.
2. Attacks with varying information about the attacked system including:
   - White box capability (i.e., knowledge of the network and all its weights or in general, the full detail of the ML employed);
   - Black box access to the system (attacker can query the system by providing input and observing the output); and
   - Blind attacks (aka, "transfer attacks"), where little is known about the system and no direct query access is possible. Though rarely considered to date, this method holds important implications for future scenarios, since it negates target defenses, which only hide the ML model used.
3. Attacks with varying information about the training data and the role of the ML system.
4. Attacks perturbing the input to the target ML system at different acquiring stages, including:
   - Perturbing the digital image already input into the target ML system (most of the current adversarial AI field); and
   - Alterations to the physical environment, e.g., placing stickers on a street sign. Physical attacks, while not extensively studied to date, are of prime importance to real systems, since they nullify target defenses that apply only to inputs already in the system.
5. Attacks on different sensory modalities such as images, videos, and audio. To date, adversarial AI has primarily considered still images, concentrating on visual inputs (cameras); increasingly, ML systems process other data modalities such as acoustic, LIDAR, and radio signals; considering only image-based inputs limits understanding of attack modalities and system vulnerabilities, leaving ML unprotected.
6. Attacks and defenses with explicit consideration of computational resources and time constraints. Current attack approaches often unrealistically assume unbounded resources. In addressing realistic conditions, some defenses will have to provide real-time protection, while others will use additional time and computational resources. Hence, GARD requires all algorithms to be analyzed and measured in terms of resource and timing constraints.
7. Detection as a form of defense. Early identification of attacks can be an effective real-time defense, allowing the system to implement countermeasures, such as closing itself from further communication and input.
8. Adaptive forms of defense. Current defense methods are fixed; utilizing a specific defense against a particular attack is of limited utility when the system is faced with multiple attacks featuring varying characteristics. A defense that can adapt itself to attack variations is considerably more robust.
9. AI deception attacks, to date, have focused on ML classifiers; GARD will consider other applications of ML, such as detection, localization, prediction, and decisions.

10. Deep networks, while popularly employed in many systems, are only one of many possible machine learning tools providing advanced capabilities; other advanced ML algorithms and techniques are within GARD's scope. Similarly, system defense solutions to protect embedded ML such as smart, active data collection will be explored in later phases.
11. Multiple deception attacks can, in principle, take place in parallel. Analogously, attacks may occur against systems that utilize multiple sensory inputs rather than only one input modality. While such attacks have yet to be introduced, they constitute a realistic scenario possibility that will be explored in later program phases.

Program evaluations will include scenarios that combine the above factors in different ways, so technical approaches should be sufficiently general to address such combinations. Biologically inspired methods may prove invaluable, yet biological fidelity is not by itself evidence for adversarial robustness. All approaches will be evaluated in terms of their success in defending AI systems, rather than contribution to computational understanding of biological systems, which is not a goal of GARD.

C. Foundations

Adversarial AI is a new field arising from very recent advances in ML. To date, defenses against AI attacks have been reactive and highly specific to particular attacks, so they lack a comprehensive theoretical foundation. GARD will lay a broad foundation for defense of advanced ML systems, including:

1. Establishing new metrics for robust generalization and for measuring different levels of vulnerabilities;
2. Identifying the primary factors underlying ML vulnerabilities. This information will be critical in fitting future AI methods to particular roles and scenarios; and
3. Enhancing completeness in algorithmic analyses by evolving methods to more accurately calculate economy of defense based on perceived cost of resources and constraints in plausible scenarios.

D. Multi-Modality

GARD will address at least three sensor modalities: 2D multichannel still images, audio, and video. All performers will be tested in the still image category, and a second modality of their choice: either audio or video categories, or, at the performer's discretion, both.

1. *2D multichannel still images.* To date, most work in adversarial AI has focused on 2D multichannel still images, but much of that work involves datasets too simple to functionally evaluate largescale ML-based defenses. GARD scenarios that involve 2D multichannel still images will use datasets on the scale of ImageNet and its successors. While RGB images are appropriate in Phase 1 of the GARD program, Phase 2 and Phase 3 will introduce alternative multichannel image modalities (e.g., RGB-depth or IR).

2. *Audio.* While some work on audio ML deception attacks exists, the literature is only a fraction of that covering image ML. At present, no physical audio attacks or defenses exist in the literature. Performers who choose audio (in addition to still images) will be

expected to propose techniques that defend against attacks on audio sound classification and speaker identification challenges. Phase 2 and Phase 3 will include defense against attacks on sound prediction and limited-dictionary speech to text.

3. *Video*. Like audio, video ML tools are currently limited. Most involve applying 2D still image approaches to video frame sequences. Performers who choose video (in addition to still images) are encouraged to utilize both spatial and temporal information in their approach. Performers choosing this modality will be expected to propose techniques that defend against attacks on object identification, classification, and localization in 3D space. Later phases will include defense against attacks on prediction as well.

GARD will rely exclusively on published attacks to enable development and evaluation of defensive technologies. It is out of scope for performers to develop novel attacks for use in advancing their research. Should there be insufficient published attacks to support proposed research at any time, the Government will negotiate appropriate changes to the statement of work.

E. Program Structure

GARD is a 48-month program, which has been divided into three phases. Phase 1 will be 12 months in duration; Phases 2 and 3 will each be 18 months long. Technical work under GARD has been organized into two technical areas (TAs):

- TA1: Defense Theories and Algorithms
  - TA1.1: Theoretical Foundations for Defensible AI
  - TA1.2: Principled Defenses
- TA2: Evaluation Framework

Each abstract and proposal submitted against this solicitation shall address only one TA. Organizations may submit multiple abstracts/proposals to any one TA, or they may propose to both TAs. TA1 proposals may address either TA1.1, TA1.2, or both.

While a proposer may submit proposals for both technical areas, a particular proposer (as identified by Commercial and Government Entity (CAGE) Code), if selected for TA1 (including either TA1.1 or TA1.2), will be unable to be selected as a performer for any portion of TA2. This selection process is intended to avoid organizational conflicts of interest (OCI) situations between the research TA and the integration and evaluation activities, as well as to ensure objective test and evaluation results.

F. Technical Areas

TA1: Defense Theories and Algorithms

Each TA1 proposal (regardless of whether focuses on TA1.1 or TA1.2, or both) will be required to:

- Address multiple ML applications, such as object detection, object localization, classification, and prediction;
- Choose between data poisoning attacks and inference attacks, or both;

- Choose either audio, video, or both to study defenses beyond 2D still images; and
- Optionally address additional modalities together with metrics and methods of evaluating the success of defenses in the new modality

TA1.1: Theoretical Foundations for Defensible AI

TA1.1 will support theoretical developments that identify underlying vulnerabilities to attack, leading to well-analyzed defense algorithms with performance bounds explicitly dependent on threat scenarios and resource constraints. Performers under this TA will be expected to show progress during each phase in at least one of the following areas:

- Creating metrics for robust generalization;
- Finding factors of vulnerability and robustness;
- Analyzing the defensibility of scenarios and algorithms; or
- Calculating economy of defense within threat scenarios.

Theory should assist in increasing depth of understanding in state-of-the-art attacks/defenses, as well as lay effective foundations for new defenses. Theories developed by TA1.1 performers must be clearly delineated and conveyed to the rest of the GARD performer groups to promote more effective analysis of ML vulnerabilities and robust generalization capabilities, enumerate attack/defense types and explore potential defenses. Algorithms developed in TA1.1 may be biologically inspired. The foundations and algorithms suggested under TA1.1 will be tested to establish their credibility and contribution to robust ML. Use of testbeds developed under TA2 is encouraged, but not required.

Proposed theories will have to account for multi-sensor, multi-modal, active, and adaptive sensors (See Table 1 below in Section I.G on metrics). "Multi-sensor" applies to either multiple sensors working in parallel or a single sensor used multiple times with resulting data fused into one coherent knowledge item (e.g., two cameras, camera plus microphone, or camera plus depth sensor). Theories should be functionally applicable to realistic scenarios and physical world attacks. Analyses should assess how a given attack scenario impacts defense method allocation of resources (e.g., computation, memory, energy consumption when available). Proposals must clarify why particular scenarios were selected, including outlining fundamental properties and relevance to well defined, realistic situations.

TA1.2: Principled Defenses

TA1.2 is the heart of the GARD program. While state-of-the-art attacks focus mainly on digitized image classification, TA1.2 performers will defend against potential detection, localization, classification, and prediction attacks. As TA1.2 projects advance in phase, performers will have to consider scenarios that allow for active / adaptive data collection by the defender system, and smart methods of using this capability to improve robustness. Additionally, recognizing attacks and identifying unsafe situations also represent important defense components to be addressed under TA1.2. Performers must indicate which scenarios their algorithms can defend against, identify breaking points, and how to maximize success of their algorithm. Figure 1 (below) provides a high-level view of the challenges and processes to be addressed in TA1.2.

Proposers may include in their technical approaches investigation of topics such as how to defend systems incorporating reinforcement learning, strategy, real-time decision making, or substantial levels of autonomy;

TA2 teams and the Government Evaluator will suggest scenarios and attacks to defend against. All performers are invited to contribute to the discussion as well. Scenarios will vary in difficulty from checking algorithm function to exploring design challenges. Evaluation scenarios will reflect current program phase foci (i.e., single sensor, multi-sensor, multimodal) and a range of possible knowledge about system attacks (e.g., blind, black-box, white-box), as well as attacks during different input acquiring stages (data set poisoning versus inference attacks). At least one physical world evaluation scenario will be conducted per phase; remaining scenarios will address digital scenarios or virtual simulations of the real world to support transition to physical scenarios. Performers will have ample notice prior to evaluation to consider different scenarios.

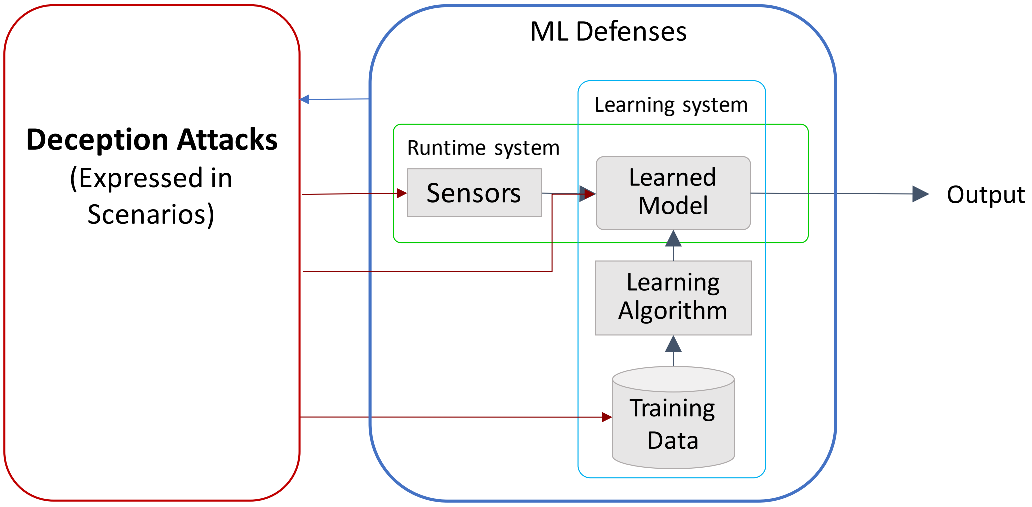


Figure 1: TA1.2 high level view of ML defense processes and challenges to meet GARD challenges.

Additional TA1.2 requirements include:

- Two to three sensor modalities must be selected:
  - One modality, 2D still images, is required
  - Performers may choose between audio, video or both as a second or second and third modality
  - Optionally one modality from the following: text, IR, LIDAR, neuromorphic spiking hardware vision system, or other similar modality of high importance. Department of Defense (DoD)-specific sensors are not the focus of GARD
- Performers will participate in both classification and prediction evaluation tasks, or both object identification and location evaluations (or all, if desired);
- Performers are encouraged to incorporate defenses to backdoor attacks (entrance without permission) induced by data poisoning that fit the modalities they choose;

- TA1.2 will be tested on a variety of scenarios; scores will be based on the level of success defending against attacks, as well as the variety of attacks and scenarios being defended against; and
- TA1.2 performers will propose their source datasets sufficient to support initial development in Phase 1, and explain their choice.

TA2: Evaluation Framework

TA2 performers will build a testbed to evaluate defenses under a wide-range of threat scenarios, and in particular, must reflect TA1.2 evaluation scenarios. The testbed will include TA1.1 metrics, as well as those designed by TA2 performer including the initial metrics discussed below. The TA2 performer will also be responsible for implementing the baseline defenses used to compute these metrics. The testbed will enable the evaluation of defense efforts against a specific set of published attacks and their combinations, including inference time and poisoning attacks, to be defined by the Government at the outset of the program, and revised periodically, in advance of evaluation events. TA2 performers will also incorporate new attacks as they are published during the program to test TA1.2 defenses, adapting them as necessary to the Evaluation Scenarios (for example, to the physical world or in black box conditions). Note, scenarios will not emulate any specific DoD operational system, but rather, will focus on essential parametrized factors central to real systems robustness. TA2 performers will be in regular contact with government evaluators for implemented attack and threat scenario details.

TA2 testbeds must include three sensor modalities: 2D multichannel still images, audio, and video. Images, videos, and audio can come from various sources, and the testbed will have to be flexible enough to support this variety. The testbed must also be flexible enough to host varied defense algorithms, and incorporate single, multiple, and multimodal sensors, as well as active and adaptive defenses and various features consistent with physical environments.

G. Metrics

The most direct measure of GARD success will be the continued improvement in model robustness to adversarial inputs compared to both (i) a system that is not under attack and without defense (baseline-not-attacked), as well as (ii) a system that is under attack and also uses current methods of defense (baseline-defended). These can be measured by comparing the reduction in accuracy induced by an attack on a system with GARD defenses to both baselines mentioned above, resulting in two metrics: Defense Figure of Merit (DFOM), and Defense Improvement over Baseline Defense (DIBD) as shown in Figure 2:

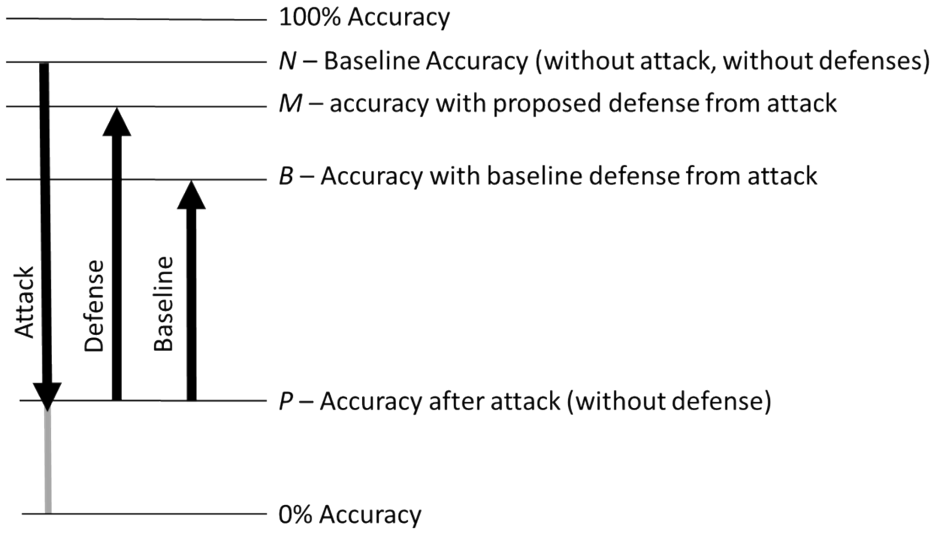

100% Accuracy
N – Baseline Accuracy (without attack, without defenses)
M – accuracy with proposed defense from attack
B – Accuracy with baseline defense from attack
Attack
Defense
Baseline
P – Accuracy after attack (without defense)
0% Accuracy

Figure 2: Components of two evaluation metrics

Auxiliary metrics defined from these components include:

- Effectiveness of new Defense = M - P
  This represents the improvement in the accuracy of the operation once the GARD defense is implemented
- Effectiveness of the Attack = N – P
- Net Defense Effectiveness = N – M
  This represents restoration of accuracy when a defense mechanism is applied after an attack. Warning: this quantity can be gamed by use of a weak attack and weak defense.
- DFOM = (M-P) / (N-P)
  This represents the "success rate" of a defense mechanism against an adversarial attack; when M = N, DFOM = 1 representing a perfect defense.
- DIBD = (M-P) / (B-P)
  This represents the "improvement" of a defense mechanism over the baseline defense under an adversarial attack; when DIBD is greater than 1 the proposed defense outperforms the baseline defense. This is the ultimate goal of defenses.

The DFOM is designed to capture the success of a defense at recovering accuracy while being subjected to adversarial attacks and may vary based on the defensibility of a scenario. The DIBD metric directly compares newly proposed defenses to known baseline defenses (e.g., the Madry defense with a perturbation size determined by the dataset). As DIBD values inherently account for the defensibility of a scenario by using a consistent baseline defense, it becomes more relevant to use DIBD to interpret a defense's performance across multiple Evaluation Scenarios.

Note that the DFOM and DIBD will vary for different random input samples. It is therefore important to present these metrics as binned ensembles (e.g., in the form of a histogram) to convey their variability. To account for statistical variability, the DFOM and DIBD targets for each Phase (see Table 1 below) must be in the 90th percentile of resulting values drawn from random input samples for a given attack.

While DFOM and DIBD serve as the primary initial metrics of robustness, GARD considers adversarial robustness as an inherently multi-objective problem. Defenses will also be evaluated using additional metrics, such as:

- *Characteristics of the attack* (e.g., whether it requires white box access, vs. working blind, how many queries it requires, or the number of poisoned samples needed);
- *Errors during defense and errors during detection*, which are the Type I, II, and III errors (over-predict, under-predict, and recover from targeted attacks) made at inference time when an attack detection mechanism is used;
- *Cost of defense in operation*, which is the computational effort, time, access and knowledge required to perform an ML operation at inference time, separating real-time from offline detection/defense;
- *Cost of defense training*, which covers the computational effort, time, access and knowledge required to train and prepare the ML system for detection of attack;
- *Computational effort*, which is quantified both as a theoretical construct via number of operations in best, average, and worst case, and by experimentation (as CPU/hours, GPU/hours, and TPU/hours) using standard computing hardware. The potential for parallelization should be explicitly noted. And finally;
- *Energy consumption,* which is a significant factor in size, weight, and power (SWAP) constrained applications.

Program goals based on the preceding explanation of metrics are expressed in Table 1 using the DFOM or DIBD metrics. Meeting, exceeding, or failing to meet goals will be considered in view of the additional metrics described above, as well as performer-suggested metrics of relevance. For example, it may be possible for a given defense mechanism to exceed a goal for a given phase, but computational resources could become too excessive to make the defense methodology practical. In short, meeting goals should be described in context to the nature of the attack, computational resources, and scenario.

Setting	Phase 1	Phase 2	Phase 3
Scenario	DFOM / DIBD	DFOM / DIBD	DFOM / DIBD
Image	>0.3/1.3	>0.7/2	>0.95/3
Sound	>0.3/1.3	>0.7/10	>0.95/100
Video	>0.3/1.3	>0.7/10	>0.95/100

Table 1: Program Defense Effectiveness Goals

H. Evaluation Scenarios

While the primary metrics DFOM and DIBD are straightforward to measure, meaningful assessment of the security implications depends on the threat context. GARD will assess defenses through a series of Evaluation Scenarios, each with a specific threat model and constraints on both attack and defense. These scenarios will be more complex and realistic than traditional adversarial examples. Many will feature physical world inputs, with complementary digital scenarios in between. Each Scenario will entail different priorities among the metrics described above; for example, placing a greater emphasis on computational costs or penalizing some types of error more than others.

The Government Evaluator will devise each scenario to be both challenging and informative about the key factors that govern model vulnerability. Scenarios are expected to cover visual and auditory modalities, initially independently. Later phases will incorporate greater complexity such as multi-sensors (e.g., two cameras), multi-modality (e.g., image plus LIDAR or depth sensors, or audio-video).

TA2 will work closely with the Government Evaluator to ensure that the testbed can support the Evaluation Scenarios. In addition, TA2 will be responsible for providing reference attacks to test TA1 defenses in each scenario. These scenarios are especially focused on TA1.2 performers, but TA1.1 teams will be encouraged to take advantage of scenario problems and TA2 testbed to test their work as well.

I. Out of Scope

The following are out of scope in this program:

- *Data theft, privacy, model inversion*: GARD is focused on attacks that induce incorrect behavior in ML models by manipulating inputs.
- *Game theory, AI strategy, agent models, or the general use of AI in adversarial contexts*: These are broad problems in themselves and more appropriate to other programs. Methods from these domains that can be shown to be relevant to the specific problems addressed by GARD are permissible.
- *Attacks on military or other government systems, extension to military datasets*: GARD is a basic research program exploring the characteristics and limitations of ML methods under general adversarial assumptions.
- *General noise robustness for ML models*: Adversarial inputs that could be ignored as having negligible probability under most noise models may be reliably produced by an attacker.
- *Generic cybersecurity of ML systems*: GARD is concerned with the specific vulnerabilities introduced by the ML model itself. Application of traditional cybersecurity analysis to systems that happen to use ML is better addressed elsewhere.
- *Methods that focus solely on attack detection*: Detection of adversarial inputs may be a useful component of defense, but does not fully address the problem.

J. Schedule, Milestones, and Evaluation

The program will conduct evaluations during each phase, as indicated in the schedule figure below (Figure 3). Performers will be evaluated twice a year in meetings; the main evaluations will be conducted toward the end of each phase, while the other evaluations near the middle of the phase will be less formal. For costing purposes, assume that meetings will alternate between the Washington D.C. area and San Francisco, CA, and that the main evaluations will require four-day-long trips, while the other evaluations will require three-day-long trips. Cost proposals should assume a kickoff date of December 1, 2019.

A Government Evaluator will develop and conduct evaluations, utilizing the TA2 performer-developed testbed and possibly adding to it. Evaluation scenario complexity will increase over the course of the program. This BAA is not soliciting for the Government Evaluator role.

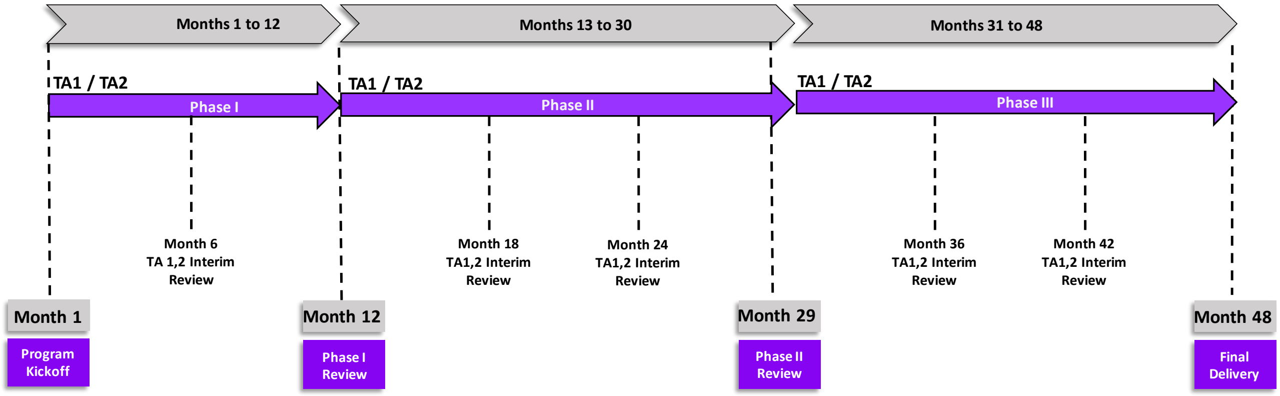


Figure 3: Overall schedule of the GARD program. Graphic assumes that GARD begins in Month 1 of a 48-month total effort.

Phase 1: (12 months) single sensor defenses

TA1.1 progress will include publishable papers describing theoretical findings, at least one of which must consider evaluation scenarios from any phase. TA1.1 progress will be assessed on their measurable contributions towards at least one of the following goals during each phase of the program: finding metrics, identifying factors of vulnerability and robustness, measuring capabilities, and relating these to existing or new algorithms. In addition, TA1.1 performers are encouraged to collaborate with performers addressing TA1.2 and consider evaluation scenarios.

TA1.2 progress will be assessed during evaluation scenarios. Scenarios will:

- include object detection, object localization, and classification with parameterized metrics for inference and poisoning attacks; TA1 will choose between defending inference and poisoning attacks;
- use 2D multichannel images, single-source audio or single-camera video;
- measure progress with previously discussed metrics (Table 1);
- involve large datasets (be prepared for ImageNet or larger);
- evaluate audio TA1 methods on sound classification and speaker identification tasks from a set of 20 speakers with the same accent and language; and
- evaluate video TA1 methods on object identification and localization.

TA2 progress will include the development of a testbed that mirrors evaluation scenarios (including ML tasks, sensor modalities, inference, and poisoning), supports the most recent published attacks, and includes all required and appropriate metrics developed by TA1.1.

Phase 2: (18 months) multi-sensor defenses

TA1.1 progress will include papers describing theoretical findings, including at least one that reflects evaluation of TA1.2 scenarios from any phase. At least one finding must be applicable to scenarios from a GARD program phase and/or sensor modality that the performer has not yet addressed, or beyond the state of the art. At least two of the papers should provide general results to the community.

TA1.2 progress will be assessed with evaluation scenarios that introduce:

- object detection, object localization, and classification and prediction;
- multi-sensor datasets (multi-camera images/videos, multi-source audio);
- increased attack capability (black-box attacks, more attack resources);
- increased performance requirements (reduced type II error/miss rate);
- combinations of state-of-the-art attacks;
- audio scenarios with multi-source audio streams;
- video scenarios with multi-view videos; and
- backdoor attacks, both poisoning and inference.

TA2 progress will include extension of the group's Phase 1 testbed to include multi-sensor datasets, support for attacks published for each evaluation scenario, and support for combination attacks.

Phase 3: (18 months) multi-modality, active, and adaptive defenses

TA1.1 progress will include papers describing theoretical findings that consider evaluation scenarios of TA1.2 from any phase with modalities or scenarios beyond the state of the art.

TA1.2 progress will be assessed with evaluation scenarios that introduce:

- object detection, object localization, and classification and prediction;
- multimodal sensors (e.g., audio + video);
- active and adaptive functionality (e.g., interactive defenses);
- increased attack capability (white-box attacks, more attack resources); and
- increased performance requirements (reduce type III error/targeting).

TA2 progress will include extension of the group's Phase 2 testbed to support Phase 3 TA1.2 evaluation scenarios, support for attacks published for each evaluation scenario, and active/adaptive functionality. Testbeds at this stage should be ready for transition.

K. Deliverables

Table 2 summarizes the anticipated deliverables by TA.

Technical Area	Anticipated Deliverables
TA1.1: Theoretical Foundations	• Properties of system design that reduce or increase vulnerability • Metrics for vulnerability, attack effectiveness • Algorithms for defense • Computational resources required for defense against a given attack • Methods for analysis of robust generalization and defended AI • Results of experiments • Bounds on reliability of test results; conclusions on effective test methods • Conclusions regarding defensibility of scenarios of interest • Recommendations on constraint conditions for TA2 challenge scenarios • Publications
TA1.2: Principled Defenses	• Implementations of existing and new defenses • Defenses and defensible ML and scenarios of success • Computational resources required for defense of a given attack scenario • Analysis – both theoretical and practical • Limits of algorithms and suggestions for defensible AI • Results of tests and competitions • Publications
TA2: Evaluation	• Testbed, in a form usable by other organizations • Definitions of new testing scenarios • Results of tests of TA1 outputs • Maintenance of a library of implemented attacks from the literature and defenses from GARD
All	• Quarterly technical status reports • Monthly financial reports • Monthly phone/video meeting with PM • Attendance at PI meetings • Support for periodic reviews • Source code and representative input data

Table 2: Deliverables

II. Award Information

A. Awards

DARPA anticipates multiple awards for TA1 and a single award for TA2. The level of funding for individual awards made under this solicitation has not been predetermined and will depend on the quality of the proposals received and the availability of funds. Awards will be made to proposers whose proposals are determined to be most advantageous to the Government, all factors considered, including the potential contributions of the proposed work, overall funding strategy, and availability of funding. See Section V for further information.

The Government reserves the right to:

- select for negotiation all, some, one, or none of the proposals received in response to this solicitation;
- make awards without discussions with proposers;
- conduct discussions with proposers if it is later determined to be necessary;
- segregate portions of resulting awards into pre-priced options;
- accept proposals in their entirety or to select only portions of proposals for award;
- fund proposals in increments and/or with options for continued work at the end of one or more phases;
- request additional documentation once the award instrument has been determined (e.g., representations and certifications); and
- remove proposers from award consideration should the parties fail to reach agreement on award terms within a reasonable time or the proposer fails to provide requested additional information in a timely manner.

Proposals selected for award negotiation may result in a procurement contract, grant, cooperative agreement, or Other Transaction (OT) depending upon the nature of the work proposed, the required degree of interaction between parties, and other factors.

Proposers looking for innovative, commercial-like contractual arrangements are encouraged to consider requesting Other Transactions. To understand the flexibility and options associated with Other Transactions, consult http://www.darpa.mil/work-with-us/contract-management#OtherTransactions.

In accordance with 10 U.S.C. § 2371b(f), the Government may award a follow-on production contract or Other Transaction (OT) for any OT awarded under this BAA if: (1) that participant in the OT, or a recognized successor in interest to the OT, successfully completed the entire prototype project provided for in the OT, as modified; and (2) the OT provides for the award of a follow-on production contract or OT to the participant, or a recognized successor in interest to the OT.

In all cases, the Government contracting officer shall have sole discretion 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 section below on Fundamental Research.

B. Fundamental Research

It is DoD policy that the publication of products of fundamental research will remain unrestricted to the maximum extent possible. National Security Decision Directive (NSDD) 189 defines fundamental research as follows:

> 'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

As of the date of publication of this BAA, the Government expects that program goals as described herein may be met by proposers intending to perform fundamental research and does not anticipate applying publication restrictions of any kind to individual awards for fundamental research that may result from this BAA. Notwithstanding this statement of expectation, the Government is not prohibited from considering and selecting research proposals that, while perhaps not qualifying as fundamental research under the foregoing definition, still meet the BAA criteria for submissions. If proposals are selected for award that offer other than a fundamental research solution, the Government will either work with the proposer to modify the proposed statement of work to bring the research back into line with fundamental research or else the proposer will agree to restrictions in order to receive an award.

Proposers should indicate in their proposal whether they believe the scope of the research included in their proposal is fundamental or not. While proposers should clearly explain the intended results of their research, the Government shall have sole discretion to select award instrument type and to negotiate all instrument terms and conditions with selectees. Appropriate clauses will be included in resultant awards for non-fundamental research to prescribe publication requirements and other restrictions, as appropriate. This clause can be found at http://www.darpa.mil/work-with-us/additional-baa.

For certain research projects, it may be possible that although the research being performed by the awardee is restricted research, a subawardee may be conducting fundamental research. In those cases, it is the awardee's responsibility to explain in their proposal why its subawardee's effort is fundamental research

C. Disclosure of Information and Compliance with Safeguarding Covered Defense Information Controls

The following provisions and clause apply to all solicitations and contracts; however, the definition of "controlled technical information" clearly exempts work considered fundamental research and therefore, even though included in the contract, will not apply if the work is fundamental research.

DFARS 252.204-7000, "Disclosure of Information"
DFARS 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls"

DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”

The full text of the above solicitation provision and contract clauses can be found at http://www.darpa.mil/work-with-us/additional-baa#NPRPAC.

Compliance with the above requirements includes the mandate for proposers to implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see https://doi.org/10.6028/NIST.SP.800-171r1) that are in effect at the time the BAA is issued.

For awards where the work is considered fundamental research, the contractor will not have to implement the aforementioned requirements and safeguards; however, should the nature of the work change during performance of the award, work not considered fundamental research will be subject to these requirements.

III. Eligibility Information

A. Eligible Applicants

DARPA welcomes engagement from all responsible sources capable of satisfying the Government's needs, including academia (colleges and universities); businesses (large, small, small disadvantaged, etc.); other organizations (including non-profit); other entities (foreign, domestic, and government); FFRDCs; minority institutions; and others.

DARPA welcomes engagement from non-traditional sources in addition to current DARPA performers.

1. Federally Funded Research and Development Centers (FFRDCs) and Government Entities

a. FFRDCs

FFRDCs are subject to applicable direct competition limitations and cannot propose to this BAA in any capacity unless they meet the following conditions: (1) FFRDCs must clearly demonstrate that the proposed work is not otherwise available from the private sector. (2) FFRDCs must provide a letter on official letterhead from their sponsoring organization citing the specific authority establishing their eligibility to propose to Government solicitations and compete with industry, and their compliance with the associated FFRDC sponsor agreement’s terms and conditions. This information is required for FFRDCs proposing to be awardees or subawardees.

b. Government Entities

Government Entities (e.g., Government/National laboratories, military educational institutions, etc.) are subject to applicable direct competition limitations. Government entities must clearly demonstrate that the work is not otherwise available from the private sector and provide written documentation citing the specific statutory authority and contractual authority, if relevant, establishing their ability to propose to Government solicitations.

c. Authority and Eligibility

At the present time, DARPA does not consider 15 U.S.C. § 3710a to be sufficient legal authority to show eligibility. While 10 U.S.C.§ 2539b may be the appropriate statutory starting point for some entities, specific supporting regulatory guidance, together with evidence of agency approval, will still be required to fully establish eligibility. DARPA will consider FFRDC and Government entity eligibility submissions on a case-by-case basis; however, the burden to prove eligibility for all team members rests solely with the proposer.

2. Foreign Participation

Non-U.S. organizations and/or individuals may participate to the extent that such participants comply with any necessary nondisclosure agreements, security regulations, export control laws, and other governing statutes applicable under the circumstances.

B. Organizational Conflicts of Interest

FAR 9.5 Requirements

In accordance with FAR 9.5, proposers are required to identify and disclose all facts relevant to potential OCIs involving the proposer's organization and *any* proposed team member (subawardee, consultant). Under this Section, the proposer is responsible for providing this disclosure with each proposal submitted to the BAA. The disclosure must include the proposer's, and as applicable, proposed team member's OCI mitigation plan. The OCI mitigation plan must include a description of the actions the proposer has taken, or intends to take, to prevent the existence of conflicting roles that might bias the proposer's judgment and to prevent the proposer from having unfair competitive advantage. The OCI mitigation plan will specifically discuss the disclosed OCI in the context of each of the OCI limitations outlined in FAR 9.505-1 through FAR 9.505-4.

Agency Supplemental OCI Policy

In addition, DARPA has a supplemental OCI policy that prohibits contractors/performers from concurrently providing Scientific Engineering Technical Assistance (SETA), Advisory and Assistance Services (A&AS) or similar support services and being a technical performer. Therefore, as part of the FAR 9.5 disclosure requirement above, a proposer must affirm whether the proposer or *any* proposed team member (subawardee, consultant) is providing SETA, A&AS, or similar support to any DARPA office(s) under: (a) a current award or subaward; or (b) a past award or subaward that ended within one calendar year prior to the proposal's submission date.

If SETA, A&AS, or similar support is being or was provided to any DARPA office(s), the proposal must include:

- The name of the DARPA office receiving the support;
- The prime contract number;
- Identification of proposed team member (subawardee, consultant) providing the support; and
- An OCI mitigation plan in accordance with FAR 9.5.

Government Procedures

In accordance with FAR 9.503, 9.504 and 9.506, the Government will evaluate OCI mitigation plans to avoid, neutralize or mitigate potential OCI issues before award and to determine whether it is in the Government's interest to grant a waiver. The Government will only evaluate OCI mitigation plans for proposals that are determined selectable under the BAA evaluation criteria and funding availability.

The Government may require proposers to provide additional information to assist the Government in evaluating the proposer's OCI mitigation plan.

If the Government determines that a proposer failed to fully disclose an OCI; or failed to provide the affirmation of DARPA support as described above; or failed to reasonably provide additional information requested by the Government to assist in evaluating the proposer's OCI mitigation plan, the Government may reject the proposal and withdraw it from consideration for award.

C. Cost Sharing/Matching

Cost sharing is not required; however, it will be carefully considered where there is an applicable statutory condition relating to the selected funding instrument (e.g., OTs under the authority of 10 U.S.C. § 2371).

D. Other Eligibility Requirements

Ability to Receive Awards in Multiple Technical Areas - Conflicts of Interest

While a proposer may submit proposals for both technical areas, a particular proposer (as identified by CAGE Code), if selected for TA1 (including either TA1.1 or TA1.2), will be unable to be selected as a performer for any portion of TA2. This selection process is intended to avoid organizational conflicts of interest (OCI) situations between the research TA and the integration and evaluation activities, as well as to ensure objective test and evaluation results.

Please note that each abstract and proposal submitted against this solicitation shall address only one TA. Organizations may submit multiple abstracts/proposals to any one TA, or they may propose to both TAs. Proposals addressing both TAs are NOT allowed. The decision as to which proposal to consider for award is at the discretion of the Government.

IV. Application and Submission Information

A. Address to Request Application Package

This document contains all information required to submit a response to this solicitation. No additional forms, kits, or other materials are needed except as referenced herein. No request for proposal (RFP) or additional solicitation regarding this opportunity will be issued, nor is additional information available except as provided at the Federal Business Opportunities website (https://www.fbo.gov), the Grants.gov website (https://www.grants.gov/), or referenced herein.

B. Content and Form of Application Submission

1. Abstracts

Proposers are encouraged to submit an abstract in advance of a proposal to minimize effort and reduce the potential expense of preparing an out of scope proposal. The abstract provides a synopsis of the proposed project, including brief answers to the following questions:

- What is the proposed work attempting to accomplish or do?
- What is the state-of-the-art, and what are the limitations?
- What are the innovations behind the proposed work?
- What milestones are to be accomplished?

DARPA will respond to abstracts with a statement as to whether DARPA is interested in the idea. If DARPA does not recommend the proposer submit a full proposal, DARPA will provide feedback to the proposer regarding the rationale for this decision. Regardless of DARPA's response to an abstract, proposers may submit a full proposal. DARPA will review all full proposals submitted using the published evaluation criteria and without regard to any comments resulting from the review of an abstract.

Abstract Format: Abstracts shall not exceed a maximum of 5 pages including the cover sheet and all figures, tables, and charts. The page limit does not include a submission letter (optional).

Reminder –Abstracts may address TA1.1 only, TA1.2 only, both TA1.1 and TA1.2, or TA2. Organizations may submit multiple abstracts to any one TA, or they may submit abstracts to multiple TAs. *Abstracts may not address both TA1 and TA2.*

All pages shall be formatted for printing on 8-1/2 by 11-inch paper with 1-inch margins and font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts. Document files must be in .pdf, .odx, .doc, .docx, .xls, or .xlsx formats. Submissions must be written in English. All pages should be numbered.

Abstracts must include the following components and page numbers:

Page 1:

- **Cover Sheet**: Provide the administrative and technical points of contact (name, address, phone, email, lead organization). Include the BAA number, title of the proposed project, primary subcontractors, estimated cost, duration of the project, and the label "Abstract."

Pages 2 to 4:

- **Goals and Impact:** Describe what is being proposed and what specific difference and effect it will make (qualitatively and quantitatively) in the field. Do not simply restate the GARD program goals. Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the relationship of this work to any other projects from the past and present. Provide preliminary results or other evidence that support likelihood of success based on your approach.
- **Technical Plan:** Outline and address the technical challenges inherent in the approach and possible solutions for overcoming potential problems. Provide appropriate specific milestones (quantitative, if possible) at intermediate stages of the project to demonstrate progress. Argue or demonstrate why your approach may be successful. The technical plan should include the following, based on the proposed Technical Area(s):
    - TA1.1
        - Key directions of theoretical exploration and justification for this choice.
        - Approach for testing the theoretical findings.
        - Potential impact of results on TA1.2 and TA2.
    - TA1.2
        - What is new in your algorithm; why should it work?
        - How does your algorithm work for physical attacks?
        - What modalities will you choose? What are the particular properties of this modality in relation to adversarial AI?
        - Suggest how your defense methods could adapt to different threat models and resource constraints.
    - TA2
        - Describe prior experience implementing and testing deception and/or poising attacks/defenses on ML systems.
        - Describe your approach to developing the software testbed to support Evaluation Scenarios.

Page 5:

- **Capabilities/Management Plan:** Provide a brief summary of the team's expertise and prior experience in this area, including that of subcontractors and key personnel. Identify a principal investigator for the project and include a description of the team's organization including roles and responsibilities.
- **Statement of Work, Cost, and Schedule:** Provide a cost estimate for resources over the proposed timeline of the project, broken down by year and subcontract (may be a rough estimate).

Additional Pages - The following, which will not impact the page count limit, should be included in the abstract:

- Brief bibliography with links to relevant papers, reports, etc.
- Concise 2-page resume of up to 3 principal personnel, covering current title and position, education, previous appointments, 5 most relevant publications, 5 secondary relevant publications, collaborations during the last 5 years, and awards.

2. Proposals

Proposals consist of Volume 1: Technical and Management Proposal (including mandatory Appendix A and optional Appendix B); Volume 2: Cost Proposal; the Level of Effort Summary by Task Excel spreadsheet; and the PowerPoint summary slide.

All pages shall be formatted for printing on 8-1/2 by 11-inch paper with 1-inch margins, single-line spacing, and a font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts. Document files must be in .pdf, .odx, .doc, .docx, .xls, or .xlsx formats. Submissions must be written in English. All pages of Volume 1 should be numbered.

A summary slide of the proposed effort, in PowerPoint format, should be submitted with the proposal. A template slide is provided as an attachment to the BAA. Submit this PowerPoint file in addition to Volumes 1 and 2 of your full proposal, and the Level of Effort Summary by Task Excel spreadsheet. This summary slide does not count towards the total page count.

Reminder – Each proposal submitted in response to this BAA shall address only TA1 or TA2, but not both. Proposals may address TA1.1 only, TA1.2 only, or both TA1.1 and TA1.2. Organizations may submit multiple proposals to any one TA, or they may propose to multiple TAs. *Proposals may not address both TA1 and TA2.*

Proposals not meeting the format prescribed herein may not be reviewed.

a. Volume 1: Technical and Management Proposal

The maximum page count for Volume 1 is 25 pages, including all figures, tables, and charts but not including the cover sheet, table of contents or appendices. A submission letter is optional and is not included in the page count. Appendix A does not count against the page limit and is mandatory. Appendix B does not count against the page limit and is optional. Additional information not explicitly called for here must not be submitted with the proposal, but may be included in the bibliography in Appendix B. Such materials will be considered for the reviewers' convenience only and not evaluated as part of the proposal.

Volume 1 must include the following components:

i. Cover Sheet: Include the following information.

- Label: "Proposal: Volume 1"
- BAA number (HR001119S0026)
- Technical Area
- Proposal title

- Lead organization (prime contractor) name
- Type of organization, selected from the following categories: Large Business, Small Disadvantaged Business, Other Small Business, HBCU, MI, Other Educational, or Other Nonprofit
- Technical point of contact (POC) including name, mailing address, telephone number, and email address
- Administrative POC including name, mailing address, telephone number, and email address
- Award instrument requested: procurement contract (specify type), grant, cooperative agreement or OT.[1]
- Total amount of the proposed effort
- Place(s) and period(s) of performance
- Other team member (subcontractors and consultants) information (for each, include Technical POC name, organization, type of organization, mailing address, telephone number, and email address)
- Proposal validity period (minimum 120 days)
- Data Universal Numbering System (DUNS) number[2]
- Taxpayer Identification Number (TIN)[3]
- Commercial and Government Entity (CAGE) code[4]
- Proposer's reference number (if any)

ii. Table of Contents

iii. Executive Summary: Provide a synopsis of the proposed project (not to exceed 2 pages), including answers to the following questions:

- What is the proposed work attempting to accomplish or do?
- What is the state-of-the-art, and what are the limitations?
- What are the innovations behind the proposed work?
- What milestones are to be accomplished?

The executive summary should include a description of the key technical challenges, a concise review of the technologies proposed to overcome these challenges and achieve the project's goal, and a clear statement of the proposed work's novelty and uniqueness.

iv. Innovative Claims and Deliverables: Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the uniqueness and benefits of this project in the context of the state of the art, alternative approaches,

[1] Information on award instruments can be found at http://www.darpa.mil/work-with-us/contract-management.

[2] The DUNS number is used as the Government's contractor identification code for all procurement-related activities. Go to http://fedgov.dnb.com/webform/index.jsp to request a DUNS number (may take at least one business day). For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa for further information.

[3] See https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin for information on requesting a TIN. Note, requests may take from 1 business day to 1 month depending on the method (online, fax, mail).

[4] A CAGE Code identifies companies doing or wishing to do business with the Federal Government. For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

and other projects from the past and present. Describe how the proposed project is revolutionary and how it significantly rises above the current state of the art. Proposers should demonstrate that they have deep knowledge of the current state of the art in the Adversarial AI area, understand the work of major players in the field, and should cite relevant work in their proposals.

Describe the deliverables associated with the proposed project and any plans to commercialize the technology, transition it to a customer, or further the work. Discuss the mitigation of any issues related to sustainment of the technology over its entire lifecycle, assuming the technology transition plan is successful.

v. Technical Plan: Outline and address technical challenges inherent in the approach and possible solutions for overcoming potential problems. Demonstrate a deep understanding of the technical challenges and present a credible (even if risky) plan to achieve the project's goal. Discuss mitigation of technical risk. Provide appropriate measurable milestones (quantitative if possible) at intermediate stages of the project to demonstrate progress and a plan for achieving the milestones. Argue or demonstrate why your approach may be successful. The technical plan should include the following, based on the proposed Technical Area(s):

- TA1.1
    - Key directions of theoretical exploration and justification for this choice.
    - Approach for testing the theoretical findings.
    - Potential impact of results on TA1.2 and TA2.
- TA1.2
    - What is new in your algorithm; why should it work?
    - How does your algorithm work for physical attacks?
    - What modalities will you choose? What are the particular properties of this modality in relation to adversarial AI?
    - Suggest how your defense methods could adapt to different threat models and resource constraints.
- TA2
    - Describe prior experience implementing and testing deception and / or poising attacks/defenses on ML systems.
    - Describe your approach to developing the software testbed to support Evaluation Scenarios.

vi. Management Plan: Provide a summary of expertise of the proposed team, including any subcontractors/consultants and key personnel who will be executing the work. Resumes count against the proposal page limit. Therefore proposers should include them in Appendix B (described below). Identify a principal investigator (PI) for the project. Provide a clear description of the team's organization including an organization chart that includes, as applicable, the relationship of team members; unique capabilities of team members; task responsibilities of team members; teaming strategy among the team members; and key personnel with the amount of effort to be expended by each person during the project. Provide a detailed plan for coordination including explicit guidelines for interaction among collaborators/subcontractors of the proposed project. Include risk management approaches. Describe any formal teaming agreements that are required to execute this project. List Government-furnished materials or data assumed to be available.

vii. Personnel, Qualifications, and Commitments: List key personnel (no more than one page per person), showing a concise summary of their qualifications, discussion of previous accomplishments, and work in this or closely related research areas. Indicate the level of effort in terms of hours to be expended by each person during each contract year and other (current and proposed) major sources of support for them and/or commitments of their efforts. DARPA expects all key personnel associated with a proposal to make a substantial time commitment to the proposed activity and the proposal will be evaluated accordingly. It is DARPA's intention to put key personnel conditions into the awards, so proposers should not propose personnel that are not anticipated to execute the award.

Include a table of key individual time commitments as follows:

Key Individual	Project	Status (Current, Pending, Proposed)	Hours on Project		
			Phase 1	Phase 2	Phase 3
Name 1	**GARD**	Proposed	x	x	x
	Project Name 1	Current	x	x	n/a
	Project Name 2	Pending	n/a	x	x
Name 2	**GARD**	Proposed	x	x	x
	Project Name 3	Proposed	x	x	x

viii. Capabilities: Describe organizational experience in relevant subject area(s), existing intellectual property, or specialized facilities. Discuss any work in closely related research areas and previous accomplishments, including prior work that will provide a starting point for the proposed research.

ix. Statement of Work (SOW): The SOW must provide a detailed task breakdown, citing specific tasks and their connection to the interim milestones and metrics, as applicable. Each year of the project should be separately defined. The SOW must not include proprietary information. For each defined task/subtask, provide:

- A general description of the objective.
- A detailed description of the approach to be taken to accomplish each defined task/subtask.
- Identification of the primary organization responsible for task execution (prime contractor, subcontractor(s), consultant(s)), by name.
- A measurable milestone, (e.g., a deliverable, demonstration, or other event/activity that marks task completion).
- A definition of all deliverables (e.g., data, reports, software) to be provided to the Government in support of the proposed tasks/subtasks.
- Identify any tasks/subtasks (by the prime or subcontractor) that will be accomplished at a university and believed to be fundamental research.

x. Schedule and Milestones: Provide a detailed schedule showing tasks (task name, duration, work breakdown structure element as applicable, performing organization), milestones, and the interrelationships among tasks. The task structure must be consistent with that in the SOW. Measurable milestones should be clearly articulated and defined in time relative to the start of the project.

xi. Appendix A: This section is mandatory and must include all of the following components. If a particular subsection is not applicable, state “NONE”. There is no page limit on Appendix A.

(1). Team Member Identification: Provide a list of all team members including the prime, subcontractor(s), and consultant(s), as applicable. Identify specifically whether any are a non-US organization or individual, FFRDC and/or Government entity. Use the following format for this list:

Individual Name	**Role (Prime, Subcontractor or Consultant)**	**Organization**	**Non-US?**		**FFRDC or Govt?**
			Org	**Ind.**	

(2). Government or FFRDC Team Member Proof of Eligibility to Propose: If none of the team member organizations (prime or subcontractor) are a Government entity or FFRDC, state “NONE”.

If any of the team member organizations are a Government entity or FFRDC, provide documentation (per Section III.A.1) citing the specific authority that establishes the applicable team member’s eligibility to propose to Government solicitations to include: 1) statutory authority; 2) contractual authority; 3) supporting regulatory guidance; and 4) evidence of agency approval for applicable team member participation.

(3). Government or FFRDC Team Member Statement of Unique Capability: If none of the team member organizations (prime or subcontractor) are a Government entity or FFRDC, state “NONE”.

If any of the team member organizations are a Government entity or FFRDC, provide a statement (per Section III.A.1) that demonstrates the work to be performed by the Government entity or FFRDC team member is not otherwise available from the private sector.

(4). Organizational Conflict of Interest Affirmations and Disclosure: If none of the proposed team members is currently providing SETA or similar support as described in Section III.B, state “NONE”.

If any of the proposed team members (individual or organization) is currently performing SETA or similar support, furnish the following information:

Prime Contract Number	DARPA Technical Office supported	A description of the action the proposer has taken or proposes to take to avoid, neutralize, or mitigate the conflict

(5). Intellectual Property (IP): If no IP restrictions are intended, state "NONE". The Government will assume unlimited rights to all IP not explicitly identified as having less than unlimited rights in the proposal.

For all noncommercial technical data or computer software that will be furnished to the Government with other than unlimited rights, provide (per Section VI.B.1) a list describing all proprietary claims to results, prototypes, deliverables or systems supporting and/or necessary for the use of the research, results, prototypes and/or deliverables. Provide documentation proving ownership or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) to be used for the proposed project. Use the following format for these lists:

NONCOMMERCIAL				
Technical Data and/or Computer Software To be Furnished With Restrictions	**Summary of Intended Use in the Conduct of the Research**	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(List)	(Narrative)	(List)	(List)	(List)
(List)	(Narrative)	(List)	(List)	(List)

COMMERCIAL				
Technical Data and/or Computer Software To be Furnished With Restrictions	**Summary of Intended Use in the Conduct of the Research**	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(List)	(Narrative)	(List)	(List)	(List)
(List)	(Narrative)	(List)	(List)	(List)

(6). Human Subjects Research (HSR): If HSR is not a factor in the proposal, state "NONE".

If the proposed work will involve human subjects, provide evidence of or a plan for review by an Institutional Review Board (IRB). For further information on this subject, see Section VI.B.2.

(7). Animal Use: If animal use is not a factor in the proposal, state "NONE".

If the proposed research will involve animal use, provide a brief description of the plan for Institutional Animal Care and Use Committee (IACUC) review and approval. For further information on this subject, see Section VI.B.2.

(8). **Representations Regarding Unpaid Delinquent Tax Liability or a Felony Conviction under Any Federal Law:** For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

Please also complete the following statements.

(1) The proposer is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability,

(2) The proposer is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(9). **Cost Accounting Standards (CAS) Notices and Certification:** For any proposer who submits a proposal which, if accepted, will result in a CAS-compliant contract, must include a Disclosure Statement as required by 48 CFR 9903.202. The disclosure forms may be found at https://www.whitehouse.gov/wp-content/uploads/2017/11/CASB_DS-1.pdf.

If this section is not applicable, state "NONE". For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

xii. Appendix B: Include a brief bibliography to relevant papers with links (when available) as well as resumes conforming to the content described above for abstract submission. This section is optional, and the materials will not be evaluated as part of the proposal review.

b. Volume 2 - Cost Proposal

This volume is mandatory and must include all the listed components. No page limit is specified for this volume.

The cost proposal should include a working spreadsheet file (.xls, .xlsx or equivalent format) that provides formula traceability among all components of the cost proposal. The spreadsheet file should be included as a separate component of the full proposal package. Costs must be traceable between the prime and subcontractors/consultants, as well as between the cost proposal and the SOW.

Pre-award costs will not be reimbursed unless a pre-award cost agreement is negotiated prior to award.

i. Cover Sheet: Include the same information as the cover sheet for Volume 1, but with the label "Proposal: Volume 2."

ii. Cost Summary Tables: Provide a single-page summary table broken down by fiscal year listing cost totals for labor, materials, other direct charges (ODCs), indirect costs (overhead, fringe, general and administrative (G&A)), and any proposed fee for the project. Include costs for each task in each fiscal year of the project by prime and major subcontractors, total cost and proposed cost share, if applicable. Provide a second table containing the same information broken down by project phase.

iii. Cost Details: For each task, provide the following cost details by month. Include supporting documentation describing the method used to estimate costs. Identify any cost sharing.

(1) Direct Labor: Provide labor categories, rates and hours. Justify rates by providing examples of equivalent rates for equivalent talent, past commercial or Government rates from a Government audit agency such as the Defense Contract Audit Agency (DCAA), the Office of Naval Research (ONR), the Department of Health and Human Services (DHHS), etc.

(2) Indirect Costs: Identify all indirect cost rates (such as fringe benefits, labor overhead, material overhead, G&A, or F&A, etc.) and the basis for each.

(3) Materials: Provide an itemized list of all proposed materials, equipment, and supplies for each year including quantities, unit prices, proposed vendors (if known), and the basis of estimate (e.g., quotes, prior purchases, catalog price lists, etc.). For proposed equipment/information technology (as defined in FAR 2.101) purchases equal to or greater than $50,000, include a letter justifying the purchase. Include any requests for Government-furnished equipment or information with cost estimates (if applicable) and delivery dates.

(4) Travel: Provide a breakout of travel costs including the purpose and number of trips, origin and destination(s), duration, and travelers per trip.

(5) Subcontractor/Consultant Costs: Provide above information for each proposed subcontractor/consultant. Subcontractor cost proposals must include interdivisional work transfer agreements or similar arrangements. If the proposer has conducted a cost or price analysis to determine reasonableness, submit a copy of this along with the subcontractor proposal.

The proposer is responsible for the compilation and submission of all subcontractor/consultant cost proposals. At a minimum, the submitted cost volume must contain a copy of each subcontractor or consultant non-proprietary cost proposal (i.e., cost proposals that do not contain proprietary pricing information such as rates, factors, etc.). Proprietary subcontractor/consultant cost proposals may be included as part of Volume 2. Proposal submissions will not be considered complete unless the Government has received all subcontractor/consultant cost proposals.

If proprietary subcontractor/consultant cost proposals are not included as part of Volume 2, they may be emailed separately to GARD@darpa.mil. Email messages must include “Subcontractor Cost Proposal” in the subject line and identify the principal investigator, prime proposer organization and proposal title in the body of the message. Any proprietary subcontractor or consultant proposal documentation which is not uploaded to the DARPA BAA Submission Website as part of the proposer's submission or provided by separate email shall be made immediately available to the Government, upon request, under separate cover (i.e., mail, electronic/email, etc.), either by the proposer or by the subcontractor/consultant organization.

Please note that a ROM or similar budgetary estimate is not considered a fully qualified subcontract cost proposal submission. Inclusion of a ROM or similar budgetary estimate, or failure to provide a subcontract proposal, will result in the full proposal being deemed non-compliant.

(6) Other Direct Costs (ODCs): Provide an itemized breakout and explanation of all anticipated ODCs.

iv. Proposals Requesting a Procurement Contract: Provide the following information where applicable.

(1) Proposals exceeding the Certification of Cost or Pricing Threshold: Provide "certified cost or pricing data" (as defined in FAR 2.101) or a request for exception in accordance with FAR 15.403.

(2) Proposals for $700,000 or more: Pursuant to Section 8(d) of the Small Business Act (15 U.S.C. § 637(d)), it is Government policy to enable small business and small disadvantaged business concerns to be considered fairly as subcontractors to organizations performing work as prime contractors or subcontractors under Government contracts, and to ensure that prime contractors and subcontractors carry out this policy. In accordance with FAR 19.702(a)(1) and 19.702(b), prepare a subcontractor plan, if applicable. The plan format is outlined in FAR 19.704.

(3) Proposers without an adequate cost accounting system: If requesting a cost-type contract, provide the DCAA Pre-award Accounting System Adequacy Checklist to facilitate DCAA's completion of an SF 1408. Proposers without an accounting system considered adequate for determining accurate costs must complete an SF 1408 if a cost type contract is to be negotiated. To facilitate this process, proposers should complete the SF 1408 found at http://www.gsa.gov/portal/forms/download/115778 and submit the completed form with the proposal. To complete the form, check the boxes on the second page, then provide a narrative explanation of your accounting system to supplement the checklist on page one.

v. Proposals Requesting an Other Transaction Agreement: Proposers must indicate whether they qualify as a nontraditional Defense contractor[5], have teamed with a nontraditional Defense contractor, or are providing a one-third cost share for this effort. Provide information to support the claims.

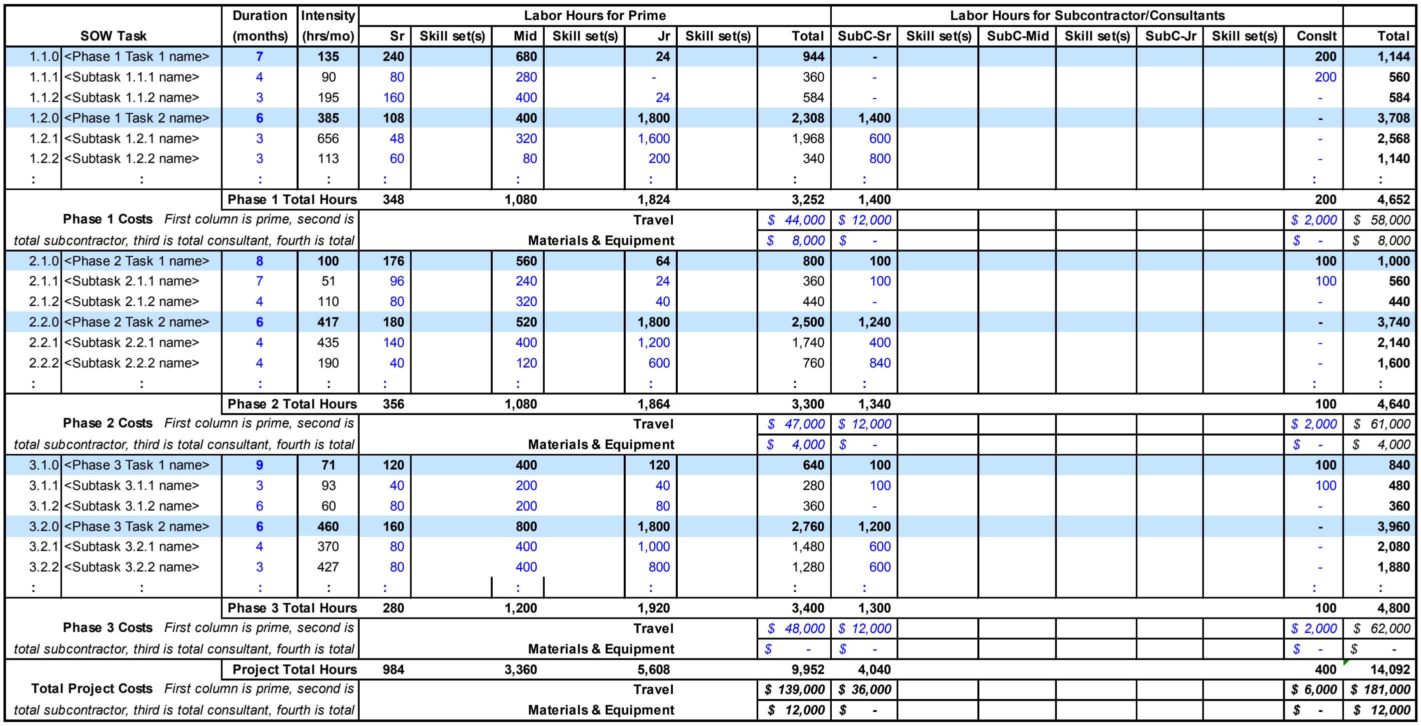
Provide a detailed list of milestones including: description, completion criteria, due date,

[5] For definitions and information on OT agreements see http://www.darpa.mil/work-with-us/contract-management.

and payment/funding schedule (to include, if cost share is proposed, contractor and Government share amounts). Milestones must relate directly to accomplishment of technical metrics as defined in the solicitation and/or the proposal. While agreement type (fixed price or expenditure based) will be subject to negotiation, the use of fixed price milestones with a payment/funding schedule is preferred. Proprietary information must not be included as part of the milestones.

c. Level of Effort Summary by Task Spreadsheet

Provide a one-page table summarizing estimated level of effort per task (in hours) broken out by senior, mid-level, and junior personnel, in the format shown below in Figure 4. Also include dollar-denominated estimates of travel, materials, and equipment. For this table, consider materials to include the cost of any data sets or software licenses proposed. For convenience, an Excel template is available for download along with the BAA. Submit the Level of Effort Summary Excel file (do not convert the Excel file to pdf format) in addition to Volume 1 and Volume 2 of your full proposal. This Excel file does not count towards the total page count.



		Duration	Intensity	Labor Hours for Prime							Labor Hours for Subcontractor/Consultants							
SOW Task		(months)	(hrs/mo)	Sr	Skill set(s)	Mid	Skill set(s)	Jr	Skill set(s)	Total	SubC-Sr	Skill set(s)	SubC-Mid	Skill set(s)	SubC-Jr	Skill set(s)	Conslt	Total
1.1.0	<Phase 1 Task 1 name>	7	135	240		680		24		944	-						200	1,144
1.1.1	<Subtask 1.1.1 name>	4	90	80		280		-		360	-						200	560
1.1.2	<Subtask 1.1.2 name>	3	195	160		400		24		584	-						-	584
1.2.0	<Phase 1 Task 2 name>	6	385	108		400		1,800		2,308	1,400						-	3,708
1.2.1	<Subtask 1.2.1 name>	3	656	48		320		1,600		1,968	600						-	2,568
1.2.2	<Subtask 1.2.2 name>	3	113	60		80		200		340	800						-	1,140
:	:	:	:	:		:		:		:	:						:	:
		Phase 1 Total Hours		348		1,080		1,824		3,252	1,400						200	4,652
Phase 1 Costs *First column is prime, second is*								Travel		$ 44,000	$ 12,000						$ 2,000	$ 58,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 8,000	$ -						$ -	$ 8,000
2.1.0	<Phase 2 Task 1 name>	8	100	176		560		64		800	100						100	1,000
2.1.1	<Subtask 2.1.1 name>	7	51	96		240		24		360	100						100	560
2.1.2	<Subtask 2.1.2 name>	4	110	80		320		40		440	-						-	440
2.2.0	<Phase 2 Task 2 name>	6	417	180		520		1,800		2,500	1,240						-	3,740
2.2.1	<Subtask 2.2.1 name>	4	435	140		400		1,200		1,740	400						-	2,140
2.2.2	<Subtask 2.2.2 name>	4	190	40		120		600		760	840						-	1,600
:	:	:	:	:		:		:		:	:						:	:
		Phase 2 Total Hours		356		1,080		1,864		3,300	1,340						100	4,640
Phase 2 Costs *First column is prime, second is*								Travel		$ 47,000	$ 12,000						$ 2,000	$ 61,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 4,000	$ -						$ -	$ 4,000
3.1.0	<Phase 3 Task 1 name>	9	71	120		400		120		640	100						100	840
3.1.1	<Subtask 3.1.1 name>	3	93	40		200		40		280	100						100	480
3.1.2	<Subtask 3.1.2 name>	6	60	80		200		80		360	-						-	360
3.2.0	<Phase 3 Task 2 name>	6	460	160		800		1,800		2,760	1,200						-	3,960
3.2.1	<Subtask 3.2.1 name>	4	370	80		400		1,000		1,480	600						-	2,080
3.2.2	<Subtask 3.2.2 name>	3	427	80		400		800		1,280	600						-	1,880
:	:	:	:	:		:		:		:	:						:	:
		Phase 3 Total Hours		280		1,200		1,920		3,400	1,300						100	4,800
Phase 3 Costs *First column is prime, second is*								Travel		$ 48,000	$ 12,000						$ 2,000	$ 62,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ -	$ -						$ -	$ -
		Project Total Hours		984		3,360		5,608		9,952	4,040						400	14,092
Total Project Costs *First column is prime, second is*								Travel		$ 139,000	$ 36,000						$ 6,000	$ 181,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 12,000	$ -						$ -	$ 12,000

Figure 4: Example level-of-effort summary table. Numbers illustrate roll-ups and subtotals. The SubC column captures all subcontractor hours and the Conslt column captures all consultant hours. The Skill set(s) columns should indicate an area of expertise (e.g., engineer, software developer, data scientist, subject matter expert).

d. Summary Slide

The submission of a PowerPoint slide summarizing the proposed effort is mandatory. A template PowerPoint slide will be provided on the Federal Business Opportunities (FedBizOpps) website, as well as on the Grants.gov website, as an attachment. Submit the PowerPoint file (do not convert PowerPoint file to pdf format) in addition to Volume 1 and Volume 2 of your full proposal. This summary slide does not count towards the total page count.

3. Proprietary and Classified Information

DARPA policy is to treat all submissions as source selection information (see FAR 2.101 and 3.104) and to disclose the 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 performing this role are expressly prohibited from performing DARPA-sponsored technical research and are bound by appropriate nondisclosure agreements.

a. Proprietary Information

Proposers are responsible for clearly identifying proprietary information. Submissions containing proprietary information must have the cover page and each page containing such information clearly marked.

b. Classified Information

Classified submissions (classified technical proposals or classified appendices to unclassified proposals) addressing any TA will not be accepted under this solicitation.

C. Submission Dates and Times

Proposers are warned that submission deadlines as outlined herein are strictly enforced. Note: some proposal requirements may take from 1 business day to 1 month to complete. See the proposal checklist in Section VIII.D for further information.

When utilizing the DARPA BAA Submission Website, as described below in Section IV.E.1 below, a control number will be provided at the conclusion of the submission process. This control number should be used in all further correspondence regarding your abstract/proposal submission.

For proposal submissions requesting cooperative agreements, Section IV.E.1.c, you must request your control number via email at GARD@darpa.mil. Please note that the control number will not be issued until after the proposal due date and time.

Failure to comply with the submission procedures outlined herein may result in the submission not being evaluated.

1. Abstracts

Abstracts must be submitted per the instructions outlined herein and received by DARPA no later than **February 26, 2019, at 12:00 noon (ET)**. Abstracts received after this date and time will not be reviewed.

2. Proposals

The proposal package -- full proposal (Volume 1 and 2) and, as applicable, proprietary subcontractor cost proposals -- must be submitted per the instructions outlined herein and received by DARPA no later than **April 11, 2019, at 12:00 noon (ET)**. Proposal submissions received after this date and time will not be reviewed.

D. Funding Restrictions

Not applicable.

E. Other Submission Requirements

1. Submission Instructions

Proposers must submit all parts of their submission package using the same method; submissions cannot be sent in part by one method and in part by another method nor should duplicate submissions be sent by multiple methods. Emailed submissions of abstracts or full proposals will not be accepted.

a. Abstracts

DARPA/I2O will employ an electronic upload submission system (https://baa.darpa.mil/) for all UNCLASSIFIED abstract responses under this solicitation. *Abstracts should not be submitted via Email or Grants.gov.*

First time users of the DARPA BAA Submission Website must complete a two-step account creation process at https://baa.darpa.mil/. The first step consists of registering for an Extranet account by going to the above URL and selecting the “Account Request” link on the right side of the page, using the Chrome browser. Upon completion of the online form, proposers will receive two separate emails; one will contain a user name and the second will provide a temporary password. Once both emails have been received, proposers must go back to the submission website and log in using that user name and password. After accessing the Extranet, proposers must create a user account for the DARPA BAA Submission Website by selecting the “Register Your Organization” link at the top of the page. The DARPA BAA Submission Website will display a list of solicitations open for submissions. Once a proposer’s user account is created, they may view instructions on uploading their abstract.

Proposers who already have an account on the DARPA BAA Submission Website may simply log in at https://baa.darpa.mil/, select this solicitation from the list of open DARPA solicitations and proceed with their abstract submission. Note: Proposers who have created a DARPA BAA Submission Website account to submit to another DARPA Technical Office’s solicitations do not need to create a new account to submit to this solicitation.

All submissions submitted electronically through DARPA's BAA website must be uploaded as zip files (.zip or .zipx extension). The final zip file should contain only the files requested herein and must not exceed 50 MB in size. Only one zip file will be accepted per submission. Note: Submissions not uploaded as zip files will be rejected by DARPA.

Please note that all submissions MUST be finalized, meaning that no further editing will be possible, when submitting through the DARPA BAA Submission Website in order for DARPA to be able to review your submission. If a submission is not finalized, the submission will not be deemed acceptable and will not be reviewed.

Website technical support may be reached at Action@darpa.mil and is typically available during regular business hours (9:00 AM – 5:00 PM ET, Monday-Friday). Questions regarding submission contents, format, deadlines, etc. should be emailed to GARD@darpa.mil.

Since abstract submitters may encounter heavy traffic on the web server, they should not wait until the day abstracts are due to request an account and/or upload the submission.

Abstracts should not be submitted via Email or Grants.gov. Any abstracts submitted by Email or Grants.gov will not be accepted or reviewed.

b. Proposals Requesting a Procurement Contract or Other Transaction

DARPA/I2O will employ an electronic upload submission system (https://baa.darpa.mil/) for UNCLASSIFIED proposals requesting award of a procurement contract or Other Transaction under this solicitation.

First time users of the DARPA BAA Submission Website must complete a two-step account creation process at https://baa.darpa.mil/. The first step consists of registering for an Extranet account by going to the above URL and selecting the “Account Request” link on the right side of the page, using the Chrome browser. Upon completion of the online form, proposers will receive two separate emails; one will contain a user name and the second will provide a temporary password. Once both emails have been received, proposers must go back to the submission website and log in using that user name and password. After accessing the Extranet, proposers must create a user account for the DARPA BAA Submission Website by selecting the “Register Your Organization” link at the top of the page. The DARPA BAA Submission Website will display a list of solicitations open for submissions. Once a proposer’s user account is created, they may view instructions on uploading their proposal.

Proposers who already have an account on the DARPA BAA Submission Website may simply log in at https://baa.darpa.mil/, select this solicitation from the list of open DARPA solicitations and proceed with their proposal submission. Note: Proposers who have created a DARPA BAA Submission Website account to submit to another DARPA Technical Office’s solicitations do not need to create a new account to submit to this solicitation.

All submissions submitted electronically through DARPA's BAA website must be uploaded as zip files (.zip or .zipx extension). The final zip file should contain only the files requested herein and must not exceed 50 MB in size. Only one zip file will be accepted per submission. Note: Submissions not uploaded as zip files will be rejected by DARPA.

Please note that all submissions MUST be finalized, meaning that no further editing will be possible, when submitting through the DARPA BAA Submission Website in order for DARPA to be able to review your submission. If a submission is not finalized, the submission will not be deemed acceptable and will not be reviewed.

Website technical support may be reached at Action@darpa.mil and is typically available during regular business hours (9:00 AM – 5:00 PM ET, Monday-Friday). Questions regarding submission contents, format, deadlines, etc. should be emailed to

GARD@darpa.mil.

Since proposers may encounter heavy traffic on the web server, it is highly recommended that proposers not wait until the day proposals are due to request an account and/or upload the submission. Full proposals should not be submitted via Email. Any full proposals submitted by Email will not be accepted or evaluated.

c. Proposals Requesting a Grant or Cooperative Agreement

Proposers requesting grants or cooperative agreements must submit proposals through one of the following methods: (1) electronic upload per the instructions at https://www.grants.gov/applicants/apply-for-grants.html; or (2) hard-copy mailed directly to DARPA. If proposers intend to use Grants.gov as their means of submission, then they must submit their entire proposal through Grants.gov; applications cannot be submitted in part to Grants.gov and in part as a hard-copy. Proposers using Grants.gov do not submit hard-copy proposals in addition to the Grants.gov electronic submission.

Submissions: Proposers must submit the three forms listed below.

SF 424 Research and Related (R&R) Application for Federal Assistance, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_SF424_2_0-V2.0.pdf. *This form must be completed and submitted.*

To evaluate compliance with Title IX of the Education Amendments of 1972 (20 U.S.C. A§ 1681 Et. Seq.), the Department of Defense is using the two forms below to collect certain demographic and career information to be able to assess the success rates of women who are proposed for key roles in applications in science, technology, engineering, or mathematics disciplines. Detailed instructions for each form are available on Grants.gov.

Research and Related Senior/Key Person Profile (Expanded), available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_KeyPersonExpanded_2_0-V2.0.pdf. *This form must be completed and submitted.*

Research and Related Personal Data, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_PersonalData_1_2-V1.2.pdf. *Each applicant must complete the name field of this form, however, provision of the demographic information is voluntary. Regardless of whether the demographic fields are completed or not, this form must be submitted with at least the applicant's name completed.*

Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. If proposers have not previously registered, this process can take between three business days and four weeks if all steps are not completed in a timely manner. See the Grants.gov user guides and checklists at https://www.grants.gov/web/grants/applicants.html for further information.

Once Grants.gov has received an uploaded proposal submission, Grants.gov will send two email messages to notify proposers that: (1) their submission has been received by Grants.gov; and (2) the submission has been either validated or rejected by the system. It may take up to two business days to receive these emails. If the proposal is rejected by Grants.gov, it must be corrected and re-submitted before DARPA can retrieve it (assuming the solicitation has not expired). If the proposal is validated, then the proposer has successfully submitted their proposal and Grants.gov will notify DARPA. Once the proposal is retrieved by DARPA, Grants.gov will send a third email to notify the proposer. If requested by the proposer, a control number for the grant/cooperative agreement submission can be provided following the due date and time for the proposals. This control number should be used in all further correspondence regarding this submission.

To avoid missing deadlines, proposers should submit their proposals to Grants.gov in advance of the proposal due date, with sufficient time to complete the registration and submission processes, receive email notifications and correct errors, as applicable.

For more information on submitting proposals to Grants.gov, visit the Grants.gov submissions page at: http://www.grants.gov/web/grants/applicants/apply-for-grants.html.

Proposers electing to submit grant/cooperative agreement proposals as hard copies must complete the SF 424 R&R form (Application for Federal Assistance, Research and Related) available on the Grants.gov website http://apply07.grants.gov/apply/forms/sample/RR_SF424_2_0-V2.0.pdf.

Proposers choosing to mail hard copy proposals to DARPA must include one paper copy and one electronic copy (e.g., CD/DVD) of the full proposal package.

Technical support for the Grants.gov website may be reached at 1-800-518-4726 and support@grants.gov. Questions regarding submission contents, format, deadlines, etc. should be emailed to GARD@darpa.mil.

V. Application Review Information

A. Evaluation Criteria

Proposals will be evaluated using the following criteria listed in descending order of importance: Overall Scientific and Technical Merit; Potential Contribution and Relevance to the DARPA Mission; and Cost Realism.

- *Overall Scientific and Technical Merit*:
  The proposed technical approach is innovative, feasible, achievable, and complete.

  The task descriptions and associated technical elements are complete and in a logical sequence, with all proposed deliverables clearly defined such that a viable attempt to achieve project goals is likely as a result of award. The proposal identifies major technical risks and clearly defines feasible mitigation efforts.

  Proposer should also take note to the information provided in Section I, as DARPA will also look at how a proposer addresses the technical challenges relevant to each TA, as well as view how key personnel will work on those challenges.

- *Potential Contribution and Relevance to the DARPA Mission:*
  The potential contributions of the proposed effort are relevant to the national technology base. Specifically, DARPA's mission is to make pivotal early technology investments that create or prevent strategic surprise for U.S. National Security.

  This includes considering the extent to which any proposed intellectual property restrictions will potentially impact the Government's ability to transition the technology.

- *Cost Realism:*

  The proposed costs are realistic for the technical and management approach and accurately reflect the technical goals and objectives of the solicitation. The proposed costs are consistent with the proposer's Statement of Work and reflect a sufficient understanding of the costs and level of effort needed to successfully accomplish the proposed technical approach. The costs for the prime proposer and proposed subawardees are substantiated by the details provided in the proposal (e.g., the type and number of labor hours proposed per task, the types and quantities of materials, equipment and fabrication costs, travel and any other applicable costs and the basis for the estimates).

B. Review and Selection Process

The review process identifies proposals that meet the evaluation criteria described above and are, therefore, selectable for negotiation of awards by the Government. DARPA policy is to ensure impartial, equitable, comprehensive proposal evaluations and to select proposals that meet DARPA technical, policy, and programmatic goals. If necessary, panels of experts in the appropriate areas will be convened. As described in Section IV, proposals must be deemed conforming to the solicitation to receive a full technical review against the evaluation criteria; proposals deemed non-conforming will be removed from consideration.

DARPA will conduct a scientific/technical review of each conforming proposal. Conforming proposals comply with all requirements detailed in this BAA; proposals that fail to do so may be deemed non-conforming and may be removed from consideration. Proposals will not be evaluated against each other since they are not submitted in accordance with a common work statement. DARPA's intent is to review proposals as soon as possible after they arrive; however, proposals may be reviewed periodically for administrative reasons.

Selections may be made at any time during the period of solicitation. Pursuant to FAR 35.016, the primary basis for selecting proposals for award negotiation shall be technical, importance to agency programs, and fund availability. Conforming proposals based on a previously submitted abstract will be reviewed without regard to feedback resulting from review of that abstract. Furthermore, a favorable response to an abstract is not a guarantee that a proposal based on the abstract will ultimately be selected for award negotiation. Proposals that are determined selectable will not necessarily receive awards.

For evaluation purposes, a proposal is defined to be the document and supporting materials as described in Section IV.B. Subject to the restrictions set forth in FAR 37.203(d), input on technical aspects of the proposals may be solicited by DARPA from non-Government consultants/experts who are strictly bound by the appropriate non-disclosure requirements. No submissions (abstract or proposal) will be returned.

VI. Award Administration Information

A. Selection Notices

After proposal evaluations are complete, proposers will be notified as to whether their proposal was selected for award negotiation as a result of the review process. Notification will be sent by email to the technical and administrative POCs identified on the proposal cover sheet. If a proposal has been selected for award negotiation, the Government will initiate those negotiations following the notification.

B. Administrative and National Policy Requirements

1. Intellectual Property

Proposers should note that the Government does not own the intellectual property of technical data/computer software developed under Government contracts; it acquires the right to use the technical data/computer software. Regardless of the scope of the Government's rights, performers may freely use their same data/software for their own commercial purposes (unless restricted by U.S. export control laws or security classification). Therefore, technical data and computer software developed under this solicitation will remain the property of the performers, though DARPA desires to have a minimum of Government Purpose Rights (GPR) to noncommercial technical data/computer software developed through DARPA sponsorship.

The program will emphasize creating and leveraging open source technology and architecture. Intellectual property rights asserted by proposers are encouraged to be aligned with open source/open architecture regimes. In particular, the testbed developed in TA2 is expected to be made available as open source.

Proposers expecting to use, but not to deliver, commercial open source tools or other materials in implementing their approach may be required to indemnify the Government against legal liability arising from such use.

All references to "Unlimited Rights" or "Government Purpose Rights" are intended to refer to the definitions of those terms as set forth in the Defense Federal Acquisition Regulation Supplement (DFARS) Part 227.

a. Intellectual Property Representations

All proposers must provide a good-faith representation of either ownership or possession of appropriate licensing rights to all other IP to be used for the proposed project. Proposers must provide a short summary for each item asserted with less than unlimited rights that describes the nature of the restriction and the intended use of the IP in the conduct of the proposed research. If proposers desire to use proprietary software or technical data or both as the basis of their proposed approach, in whole or in part, they should: (1) clearly identify in Appendix A such software/data and its proposed particular use(s); (2) explain how the Government will be able to reach its program goals (including transition) within the proprietary model offered; and (3) provide possible nonproprietary alternatives in any area that might present transition difficulties or increased risk or cost to the Government under the proposed proprietary solution.

b. Patents

All proposers must include documentation proving ownership or possession of appropriate licensing rights to all patented inventions to be used for the proposed project. If a patent application has been filed for an invention, but it includes proprietary information and is not publicly available, a proposer must provide documentation that includes: the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and summary of the patent title, with either: (1) a representation of invention ownership, or (2) proof of possession of appropriate licensing rights in the invention (i.e., an agreement from the owner of the patent granting license to the proposer).

c. Procurement Contracts

- **Noncommercial Items (Technical Data and Computer Software):** Proposers requesting a procurement contract must list all noncommercial technical data and computer software that it plans to generate, develop, and/or deliver, in which the Government will acquire less than unlimited rights and to assert specific restrictions on those deliverables. In the event a proposer does not submit the list, the Government will assume that it has unlimited rights to all noncommercial technical data and computer software generated, developed, and/or delivered, unless it is substantiated that development of the noncommercial technical data and computer software occurred with mixed funding. If mixed funding is anticipated in the development of noncommercial technical data and computer software generated, developed, and/or delivered, proposers should identify the data and software in question as subject to GPR. In accordance with DFARS 252.227-7013, “Rights in Technical Data - Noncommercial Items,” and DFARS 252.227-7014, “Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation,” the Government will automatically assume that any such GPR restriction is limited to a period of 5 years, at which time the Government will acquire unlimited rights unless the parties agree otherwise. The Government may use the list during the evaluation process to evaluate the impact of any identified restrictions and may request additional information from the proposer, as may be necessary, to evaluate the proposer’s assertions. Failure to provide full information may result in a determination that the proposal is not compliant with the solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

- **Commercial Items (Technical Data and Computer Software):** Proposers requesting a procurement contract must list all commercial technical data and commercial computer software that may be included in any deliverables contemplated under the research project, and assert any applicable restrictions on the Government’s use of such commercial technical data and/or computer software. In the event a proposer does not submit the list, the Government will assume there are no restrictions on the Government’s use of such commercial items. The Government may use the list during the evaluation process to evaluate the impact of any identified restrictions and may request additional information from the proposer to evaluate the proposer’s assertions. Failure to provide full information may result in a determination that the proposal is not compliant with the solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

d. Other Types of Awards

Proposers responding to this solicitation requesting an award instrument other than a procurement contract shall follow the applicable rules and regulations governing those award instruments, but in all cases should appropriately identify any potential restrictions on the Government's use of any intellectual property contemplated under those award instruments in question. This includes both noncommercial items and commercial items. The Government may use the list as part of the evaluation process to assess the impact of any identified restrictions and may request additional information from the proposer, to evaluate the proposer's assertions. Failure to provide full information may result in a determination that the proposal is not compliant with the solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

2. Human Research Subjects/Animal Use

Proposers that anticipate involving Human Research Subjects or Animal Use must comply with the approval procedures detailed at http://www.darpa.mil/work-with-us/additional-baa.

3. Electronic and Information Technology

All electronic and information technology acquired through this solicitation must satisfy the accessibility requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 794d) and FAR 39.2. Each project involving the creation or inclusion of electronic and information technology must ensure that: (1) Federal employees with disabilities will have access to and use of information that is comparable to the access and use by Federal employees who are not individuals with disabilities; and (2) members of the public with disabilities seeking information or services from DARPA will have access to and use of information and data that is comparable to the access and use of information and data by members of the public who are not individuals with disabilities.

4. System for Award Management (SAM) and Universal Identifier Requirements

All proposers must be registered in SAM unless exempt per FAR 4.1102. FAR 52.204-7, "System for Award Management" and FAR 52.204-13, "System for Award Management Maintenance" are incorporated into this BAA. See http://www.darpa.mil/work-with-us/additional-baa for further information.

International entities can register in SAM by following the instructions in this link: https://www.fsd.gov/fsd-gov/answer.do?sysparm_kbid=dbf8053adb119344d71272131f961946&sysparm_search=KB0013221.

Note that new registrations can take an average of 7-10 business days to process in SAM. SAM registration requires the following information:

- DUNS number
- TIN
- CAGE Code. If a proposer does not already have a CAGE code, one will be assigned during SAM registration.
- Electronic Funds Transfer information (e.g., proposer's bank account number, routing

number, and bank phone or fax number).

5. Publication of Grant Awards

Per Section 8123 of the Department of Defense Appropriations Act, 2015 (Pub. L. 113-235), all grant awards must be posted on a public website in a searchable format. To comply with this requirement, proposers requesting grant awards must submit a maximum one (1) page abstract that may be publicly posted and explains the program or project to the public. The proposer should sign the bottom of the abstract confirming the information in the abstract is approved for public release. Proposers are advised to provide both a signed PDF copy, as well as an editable (e.g., Microsoft word) copy. Abstracts contained in grant proposals that are not selected for award will not be publicly posted.

C. Reporting

1. Technical and Financial Reports

The number and types of technical and financial reports required under the contracted project will be specified in the award document, and will include, at a minimum, monthly financial status reports and a quarterly technical status summary. A final report that summarizes the project and tasks will be required at the conclusion of the performance period for the award. The reports shall be prepared and submitted in accordance with the procedures contained in the award document.

2. Representations and Certifications

If a procurement contract is contemplated, prospective awardees will need to be registered in the SAM database prior to award and complete electronic annual representations and certifications consistent with FAR guidance at 4.1102 and 4.1201; the representations and certifications can be found at www.sam.gov. Supplementary representations and certifications can be found at http://www.darpa.mil/work-with-us/additional-baa.

.

3. Wide Area Work Flow (WAWF)

Unless using another means of invoicing, performers will be required to submit invoices for payment directly at https://wawf.eb.mil. If applicable, WAWF registration is required prior to any award under this solicitation.

4. Terms and Conditions

A link to the DoD General Research Terms and Conditions for Grants and Cooperative Agreements and supplemental agency terms and conditions can be found at http://www.darpa.mil/work-with-us/contract-management#GrantsCooperativeAgreements.

5. FAR and DFARS Clauses

Solicitation clauses in the FAR and DFARS relevant to procurement contracts and FAR and DFARS clauses that may be included in any resultant procurement contracts are incorporated herein and can be found at www.darpa.mil/work-with-us/additional-baa.

See also Section II.C regarding the disclosure of information and compliance with safeguarding covered defense information controls (for FAR-based procurement contracts only).

6. i-Edison

Award documents will contain a requirement for patent reports and notifications to be submitted electronically through the i-Edison Federal patent reporting system at http://s-edison.info.nih.gov/iEdison.

7. Controlled Unclassified Information (CUI) on Non-DoD Information Systems

Further information on Controlled Unclassified Information on Non-DoD Information Systems is incorporated herein can be found at www.darpa.mil/work-with-us/additional-baa.

VII. Agency Contacts

DARPA will use email for all technical and administrative correspondence regarding this solicitation.

- **Technical POC:** Dr. Hava Siegelmann, Program Manager, DARPA/I2O

- **Email:** GARD@darpa.mil

- **Mailing address**:
  DARPA/I2O
  ATTN: HR001119S0026
  675 North Randolph Street
  Arlington, VA 22203-2114

- **I2O Solicitation Website:** http://www.darpa.mil/work-with-us/opportunities

VIII. Other Information

A. Frequently Asked Questions (FAQs)

Administrative, technical, and contractual questions should be sent via email to GARD@darpa.mil. 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 7 days of closing may not be answered. If applicable, DARPA will post FAQs to http://www.darpa.mil/work-with-us/opportunities under the GARD program.

B. Proposers Day

The GARD Proposers Day will be held on February 6, 2019, in Arlington, VA. The special notice regarding the GARD Proposers Day, DARPA-SN-19-25, can be found at https://www.fbo.gov/index?s=opportunity&mode=form&id=ef88d2693ffeb577b70ebf4b85d9094b&tab=core&_cview=0.

For further information regarding the GARD Proposers Day, including slides and a video from the event, please see http://www.darpa.mil/work-with-us/opportunities under HR001119S0026.

C. Submission Checklist

The following items apply prior to proposal submission. Note: some items may take up to 1 month to complete.

✓	Item	BAA Section	Applicability	Comment
	Abstract	IV.B.1	Optional, but recommended	Conform to stated page limit.
	Obtain DUNS number	IV.B.2.a.i	Required of all proposers	The DUNS Number is the Federal Government's contractor identification code for all procurement-related activities. See http://fedgov.dnb.com/webform/index.jsp to request a DUNS number. Note: requests may take at least one business day.
	Obtain Taxpayer Identification Number (TIN)	IV.B.2.a.i	Required of all proposers	A TIN is used by the Internal Revenue Service in the administration of tax laws. See https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin for information on requesting a TIN. Note: requests may take from 1 business day to 1 month depending on the method (online, fax, mail).
	Register in the System for Award Management (SAM)	VI.B.4	Required of all proposers	The SAM combines Federal procurement systems and the Catalog of Federal Domestic Assistance into one system. See https://sam.gov/SAM/ for information and registration. Note: new registrations can take an average of 7-10 business days. SAM registration requires the following information: -DUNS number -TIN -CAGE Code. A CAGE Code identifies companies doing or wishing to do business with the Federal Government. If a proposer does not already have a CAGE code, one will be assigned

				during SAM registration. -Electronic Funds Transfer information (e.g., proposer's bank account number, routing number, and bank phone or fax number).
	Ensure eligibility of all team members	III	Required of all proposers	Verify eligibility, as applicable, for in accordance with requirements outlined in Section 3.
	Register at Grants.gov	IV.E.1.c	Required for proposers requesting grants or cooperative agreements	Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. If proposers have not previously registered, this process can take between three business days and four weeks if all steps are not completed in a timely manner. See the Grants.gov user guides and checklists at https://www.grants.gov/web/grants/applicants.html for further information.

The following items apply as part of the submission package:

✓	Item	BAA Section	Applicability	Comment
	Volume 1 (Technical and Management Proposal)	IV.B.2	Required of all proposers	Conform to stated page limits and formatting requirements. Include all requested information.
	Appendix A	IV.B.2.a.xi	Required of all proposers	-Team member identification - Government/FFRDC team member proof of eligibility - Organizational conflict of interest affirmations - Intellectual property assertions - Human subjects research - Animal use - Unpaid delinquent tax liability/felony conviction representations -CASB disclosure, if applicable
	Appendix B	IV.B.2.a.xii	Optional of all proposers	- Appendix B does not count against the page limit - A brief bibliography to relevant papers, reports, or resumes - Do not include technical papers - The materials in Appendix B will not be evaluated as part of the proposal review
	Volume 2 (Cost Proposal)	IV.B.2.b	Required of all proposers	- Cover Sheet - Cost summary - Detailed cost information including justifications for direct labor, indirect costs/rates, materials/equipment, subcontractors/consultants, travel, ODCs - Cost spreadsheet file (.xls or equivalent format) - If applicable, list of milestones for OTs - Subcontractor plan, if applicable Subcontractor cost proposals - Itemized list of material and equipment items to be purchased with vendor quotes or engineering estimates for material and equipment more than $50,000 - Travel purpose, departure/arrival destinations, and sample airfare
	Level of Effort Summary by Task Excel spreadsheet	IV.B.2.c	Required of all proposers	A template LoE Excel file will be provided on the FedBizOpps website as an attachment. Submit the LoE Excel file (do not convert Excel file to pdf format).

	PowerPoint Summary Slide	IV.B.2.d	Required of all proposers	A template PowerPoint slide will be provided on the FedBizOpps website as an attachment. Submit the PowerPoint file (do not convert PowerPoint file to pdf format).

For information concerning agency level protests see http://www.darpa.mil/work-with-us/additional-baa#NPRPAC.