Broad Agency Announcement

Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)

INFORMATION INNOVATION OFFICE

HR001121S0040

September 20, 2021

TABLE OF CONTENTS

PART I: OVERVIEW INFORMATION 3
PART II: FULL TEXT OF ANNOUNCEMENT 4
I. Funding Opportunity Description 4
II. Award Information 22
A. General Award Information 22
Fundamental Research 23
III. Eligibility Information 24
A. Eligible Applicants 24
B. Organizational Conflicts of Interest 25
C. Cost Sharing/Matching 26
IV. Application and Submission Information 26
A. Address to Request Application Package 26
B. Content and Form of Application Submission 26
V. Application Review Information 39
A. Evaluation Criteria 39
B. Review of Proposals 40
VI. Award Administration Information 41
A. Selection Notices and Notifications 41
B. Administrative and National Policy Requirements 41
C. Reporting 42
D. Electronic Systems 42
E. DARPA Embedded Entrepreneur Initiative (EEI) 42
VII. Agency Contacts 44
VIII. Other Information 44
IX. APPENDIX 1 – PROPOSAL SUMMARY SLIDE 46

PART I: OVERVIEW INFORMATION

- **Federal Agency Name** – Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)
- **Funding Opportunity Title** – Hardening Development Toolchains Against Emergent Execution Engines (HARDEN)
- **Announcement Type** – Initial announcement
- **Funding Opportunity Number** – HR001121S0040
- **Catalog of Federal Domestic Assistance Numbers (CFDA)** – 12.910 Research and Technology Development
- **Dates**
  - Posting Date: September 20, 2021
  - Proposers Day: September 30, 2021
  - Questions Due: November 1, 2021, 12:00 noon, Eastern Time
  - Proposal Due Date: November 4, 2021, 12:00 noon, Eastern Time
  - Solicitation Closing Date: March 21, 2022, 5:00 pm, Eastern Time
- **Program Overview** – The HARDEN program will explore novel approaches that use formal verification methods and Artificial Intelligence (AI)-aided program models, analyses, and logics to develop practical tools to anticipate, isolate, and mitigate emergent execution engines throughout the entire software development lifecycle in order to disrupt the patterns of robust, reliable, and composable exploit primitives that empower attackers.
- **Anticipated Individual Awards** – There are multiple technical areas for this solicitation. Multiple awards are anticipated in Technical Area 1 and Technical Area 2, and a single award is anticipated in Technical Area 3 and Technical Area 4.
- **Types of Instruments that May be Awarded** – Procurement Contracts, Cooperative Agreements, or Other Transactions (OT)
- **Agency Contacts**
  - Points of Contact

    The BAA Coordinator for this effort can be reached at:
    Email: HARDEN@darpa.mil.
    DARPA/I2O
    ATTN: HR001121S0040
    675 North Randolph Street
    Arlington, VA 22203-2114

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

This publication constitutes a Broad Agency Announcement (BAA) as contemplated in Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016 and 2 C.F.R. § 200.203. Any resultant award negotiations will follow all pertinent laws and regulations, and any negotiations and/or awards for procurement contracts will use procedures under FAR 15.4, Contract Pricing, as specified in the BAA.

The Defense Advanced Research Projects Agency (DARPA) is soliciting innovative proposals in the following areas of interest: tools to anticipate, isolate, and mitigate adversarially programmable emergent behaviors in integrated software systems, and tools to protect intended software abstractions from adversarial reuse. Proposed research should investigate innovative approaches that enable revolutionary advances in theory, tools, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

A. Program Overview

Introduction

The Department of Defense (DoD) has a critical need to deny cyber attackers the capability to execute unintended, yet robust and often unobservable computations on DoD systems and critical infrastructure systems. The Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program will explore novel theories and approaches, and develop practical tools to anticipate, isolate, and mitigate emergent behaviors in computing systems throughout the entire software development lifecycle (SDLC). HARDEN will radically improve security outcomes in software for integrated systems by creating novel tools, metadata, and instrumentation for emergent computation, and it will efficiently mitigate exploitation of software abstractions and protect intended abstractions from adversarial reuse. HARDEN will integrate those capabilities into the standard processes of the SDLC.

Empirically, modern exploitation methods rely on long chains of emergent behaviors of the target's unprotected computational abstractions, where attackers leverage one combination of abstractions to create an ephemeral state in which the next set of unprotected abstractions is exposed, until the goals of exploitation are achieved. Counterintuitively, instead of being brittle and easily disrupted, these chains are robust and portable between implementations independently created by different vendors. This phenomenon is colloquially described as "weird machines"—well-defined, robust, and abstractable engines of emergent execution (EE) and adversarial programmability—already pre-existing within the target and being merely unlocked for an attacker's use through coding flaws.

Removal of individual code flaws by initial fixes and mitigations tends to be ineffective against methodical exploit programming because such fixes typically fail to disrupt the underlying

emergent execution engine or "weird machine," which remains accessible to the attackers through other flaws.

The HARDEN program will use formal verification methods and Artificial Intelligence (AI)-aided program models, analyses, and logics to develop practical tools to prevent exploitation of emergent execution engines by disrupting the patterns of robust, reliable exploits used by attackers.

HARDEN tools will facilitate analyses of integrated systems by leveraging modeling and analysis of multi-layered software abstractions, their interactions, and emergent properties. HARDEN tools will analyze the extent of protection of each layer of abstraction and the semantic anchorings in lower layers to reason about its propensity for adversarial programmability and EE. Based on these analyses, the tools will alert system designers and developers about designs and implementations likely to result in adversarially programmable emergent behaviors. HARDEN tools will also suggest semantically equivalent transformations of implementations to mitigate composability of emergent behaviors and to disrupt exploit programming. Additionally, HARDEN tools will help validate both the design and implementation of integrated systems and inform architectural security standards for systems-of-systems.

To accomplish these goals, the HARDEN program will leverage the insight that composability of emergent behaviors and unprotected abstractions yield key advantages for the attacker. Composability allows the attacker to create resilient programs out of sequences of emergent behaviors, chaining exploit primitives even where security mitigations reduce the effects of any single behavior or flaw. HARDEN's insight is that unintended composability of the systems' own abstractions and emergent behaviors is what enables attackers to robustly and effectively drive the system through long series of unintended illegal states without crashing or manifesting other observable signs of misbehavior.

The program seeks breakthrough approaches to the following technical challenges, including but not limited to:

- Overcoming state explosion of typical models of software behavior;
- Making annotation of expected behavior and predictions of emergent behavior accessible to typical software developers;
- Developing efficient means of communicating about EE with software architects and developers;
- Anticipating and preventing potential EE within common developer workflows and tools;
- Creating models of EE that capture designed-in EE and abstract away irrelevant parts of the implementation;
- Modeling interfaces and Application Programming Interfaces (APIs) at several layers of abstraction, together with the interactions between these layers; and,
- Developing effective tiered representations of abstractions to reason about EE and formats, and to efficiently store and retrieve these representations alongside software deliverables (e.g., by extending symbolic debugging data formats).

The HARDEN program will focus on validating approaches by applying broad theories and generic tools to concrete technological use cases of integrated software systems described in this BAA, with the overall goal of producing comprehensive security improvements in these systems as a whole.

Background

Today's software development pipelines and testing methodologies do not typically include tools for reasoning about adversarial reuse of code that was correct for its original purpose. This leads to unwitting creation of stable, reliable patterns of emergent behaviors within integrated software systems that lend themselves to adversarial programming by attackers. Attackers have demonstrated an increasing ability to compose emergent behaviors of target systems into unintended and "weird," yet effective and robust, exploit programming models and execution engines. Some examples are: a) modern web browser exploits co-opt functionality of the browser's sophisticated memory management algorithms and just-in-time compilation of web scripts; b) the Spectre family of exploits adversarially reuse the Central Processing Unit's (CPU's) microarchitecture and transactional memory mechanisms; and c) modern bootkits leverage elements of the trusted computing system management modes. In each case, attackers try to program an already present unintended engine of emergent behaviors with a sequence of suitable macro- or micro-events.

Since today's developer tools focus only on intended execution paths and limited deviations from these paths, the developers remain unaware of designed-in emergent execution behaviors and adversarial reprogramming modes of their products for years after their release. Even when advanced exploitation models based on these behaviors are made public, creating effective mitigations takes years, as these mitigations need to consider widely used designed-in features rather than random developer errors.

Today, the software industry uses two approaches to experimentally characterize emergent behaviors in finished products: *fuzz-testing* (a.k.a. fuzzing) and *Chaos Engineering*. Fuzzing subjects the system-under-test to randomly generated malformed inputs and records violations of intended behaviors (such as crashes or out-of-bound memory accesses), while selecting or mutating inputs to maximize observed program coverage. Security researchers then manually analyze elicited violations for composability and judge whether they enable general patterns of programmability by the adversary. Fuzzing operates on the compiled binary form of the software product—in essence, the lowest form of computing abstraction above hardware, which is forgetful of most higher-level abstractions. Google and Microsoft's recently open-sourced fuzzing infrastructures enable testing of individual code units rather than finished products, as they both recognize the effectiveness of fuzz-testing for finding code flaws.

Chaos Engineering operates at the highest form of architectural abstractions in distributed systems, such as services, nodes, or network functions, subjecting their instances to simulated random disconnections or excessive latency. Chaos Engineering eschews simulating data corruption (such as fuzzing), as it focuses on availability at scale regardless of the root causes of individual node failures.

Additionally, the industry is starting to adopt formal methods to ensure that the code behaves according to its specifications. However, today's formal methods do not characterize behaviors of code that are outside the specifications, nor do they reveal behavior in the presence of violations of specification assumptions. Without the ability to represent or discover intermediate and implicit abstractions involved in implementations, today's formal methods cannot help explore their composition properties, the resulting EE modes, and the adversarial programming models of their unintended reuse by attackers.

HARDEN will offer efficient mitigation at the early SDLC stages and protection of intended software abstractions from adversarial reuse. HARDEN will instrument the development toolchain to provide reasoning about emergent behaviors at all available layers of abstraction, from the compiled binary code through the compiler abstractions and intermediate representations, to the highest levels of architectural abstraction. It will develop metadata representations, logics, symbolic and binary instrumentation, as well as developer-focused tooling integrated with the standard build chains and integrated development environments (IDEs) to warn the designer and the developer about potential emergent behaviors at their inception point.

Insufficiency of Current Approaches

Neither fuzzing nor Chaos Engineering provide ways to reason about emergent behaviors at their inception. Both methods are limited to the lowest and the highest levels of architectural abstraction, and fail to exploit architectural knowledge of the intermediate abstraction layers in integrated systems. Neither method explores the composability of emergent behaviors.

These limitations are crucial. Prior studies have demonstrated that reliable adversarial reuse of code is enabled in multi-layered systems by particular implementations of higher-level abstractions via intermediate abstractions. Exploits leverage unintended, emergent, but fairly general and resilient abstractions impressed onto lower system layers by systematic design choices inherent in the target itself or in the development toolchain. Abuse of these impressions, known as "leaky abstractions," is what lends exploitation methodologies their resilience and portability between platforms, despite the many low-level differences between these platforms. What makes exploitation methodologies teachable and their mitigation hard is that disrupting the unintended abstractions that an exploit relies upon must be done without disrupting the intended design.

For example, the Return-Oriented Programming (ROP) exploit relies on the design of the stack activation frames (an intermediate compiler abstraction). Other exploits such as Jump Oriented Programming (JOP), Signal Return Oriented Programming (SROP), and Counterfeit Object Oriented Programming (COOP) rely on indirect control flow abstractions created by compilers or systems' libraries. Heap memory manipulation techniques, "heap grooming" or "heap Feng-shui," use abstractions of the heap metadata originating in the design, metadata operations, and memory management algorithms. This is why these techniques are effective with small variations across different instruction-set architectures and operating systems. Similarly, exploits leveraging CPU microarchitectures and chains-of-trust rely on intermediate abstractions of these

designs and therefore persist across architectures. This way, the exploits can be modeled without regard to the details of specific target microarchitectures or chipset implementations.

Empirically, even the best-of-breed fuzzing methods fail to uncover flaws in software layers not immediately adjacent to the interface through which attackers inject their crafted inputs. This happens because the fuzzer's guiding algorithm must essentially re-discover intended code paths, data structures, and other interfaces at great cost, and with little to no knowledge of the underlying abstractions. For that same reason, even when fuzzing triggers emergent behaviors in higher layers, it cannot reason about its composition.

Without the ability to model, represent, and discover intermediate abstractions inherent in designs and implementations, today's methods, including formal verification methods, cannot explore their composition properties, the resulting EE modes, and the adversarial programming models of the unintended reuse by attackers.

Program Scope

HARDEN tools will facilitate modeling and analysis of integrated systems with technological stacks including, but not limited to, the following:

- Instrumentation of the development toolchain for reasoning about EE behaviors at all available layers of abstraction;
- Capabilities for effective searching and automated reasoning about EE behaviors for a wide variety of higher-layer abstractions, generalizing recent methods for reasoning about unintended behaviors without complete knowledge of implementations; and
- Prevention of composability of EE behaviors underlying robust exploit chain construction.

HARDEN tools for integrated systems will produce assurance evidence and trustworthiness outcomes superior to those of the current approaches of fuzz-testing and Chaos Engineering.

Although HARDEN seeks to create broad theories and generic tools, the program will focus on validating its approaches by applying them to concrete technological use cases of integrated software systems described further under "Technological Use Cases" within Section I.B.

B. Program Structure

The program will produce theories, technologies, tools, and formal methodologies leading to experimental prototype(s) that provide capabilities for the mitigation of emergent behaviors throughout the software lifecycle in order to improve security outcomes in software for complex integrated systems. It is expected that these prototypes will provide a starting point for technology transition and demonstrate that chained exploits can be impeded by disrupting them at all levels of abstraction in mission-critical software.

The HARDEN program is a 48-month program organized into three phases: Phases 1 and 2 will each be 18-months, followed by a 12-month Phase 3. Each of the Phases' Metrics are described

in Table 1 under Section I.C.

The program is divided into four Technical Areas (TAs) to support program goals:

- TA1: Tooling for developers
- TA2: Modeling of emergent behaviors
- TA3: Voice of the offense
- TA4: Integration and systems engineering evaluation

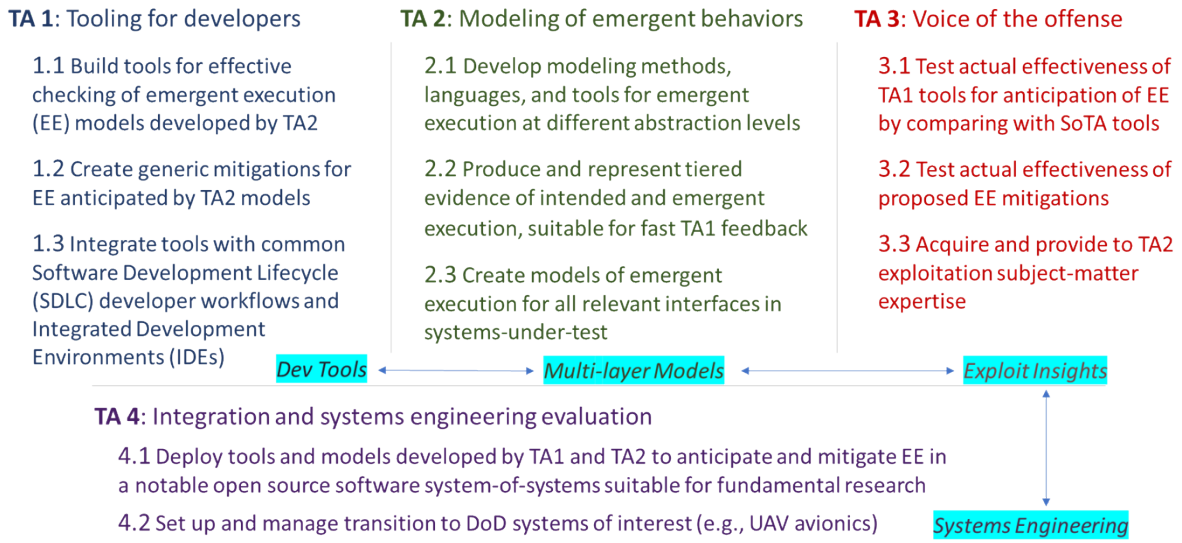

Figure 1: HARDEN TAs 1-4 with notional subtasks and challenges

DARPA anticipates funding multiple technical approaches and performers across the HARDEN technical areas. Beyond Phase 1, subsequent phases will be considered options, and may or may not be exercised at the sole discretion of the Government. Funding of options will be based on demonstrated technical progress towards the goals of the HARDEN program and availability of funding.

Within the program phases, proposers are encouraged to identify a compact viable core subset of their proposed technologies and then associate them to proposal options that increase the practical coverage of the technological use cases discussed in "Technological Use Cases" and "Exemplary Evaluation and Transition Use Cases" within this section. These optional add-ons may or may not be exercised at the sole discretion of the Government.

TA1 and TA2 performers should be prepared to work closely with each other in order to support the integration of the TA1 tools for effective checking of EE models developed by TA2, and for TA1 tools that create effective mitigations for EE anticipated by the TA2 models. In addition, TA2 and TA3 performers should be prepared to work closely with each other, in order to ensure that TA2's models reflect TA3's insights of edge-of-the-art exploitation and enhance these insights.

To facilitate the open exchange of information, performers will have Associate Contractor Agreement (ACA) language included in their award, which is described further in Section VIII. The TA4 performers will be responsible for executing the HARDEN ACA. While TA4 performers will be a party to the ACA, it is expected that TA4 outputs will be largely independent of TA1, TA2, and TA3 work, although robust interaction is expected.

Each proposal may address any one TA, or a combination of TA1 and TA2. Proposals covering a combination of TA1 and TA2 must make the respective efforts and costs proposed on the different TAs **clearly separable** to enable partial awards, and should explain their rationale for combining these two TAs, and their collaboration plans with the other TAs. Significant cost reductions for the combined TA1 and TA2 effort will be expected through synergies of the proposed approaches.

Proposers may submit multiple proposals. The Government reserves the right to decide which, if any, are selected for award. A proposer submitting combined TA1 and TA2 proposals may be selected to perform on one, or both, of these TAs. A proposer submitting proposals to TA3 and some other TA(s), if selected to perform on TA3, cannot be selected to perform on any other TAs, whether as a prime, subcontractor, or any other capacity from an organizational to individual level, to protect the integrity of the program evaluation. Similarly, a proposer submitting proposals to TA4 and some other TA(s), if selected to perform on TA4, cannot be selected to perform on any other TAs, whether as a prime, subcontractor, or any other capacity from an organizational to individual level.

DARPA encourages proposers to consider the investigation and creation of open-source and free software approaches. DARPA strongly encourages that proposals provide an overall open-source HARDEN framework that will result in open, modular tool architectures. Restricting technology transition of a proposed HARDEN technology may be considered a weakness of the proposal and DARPA believes that open-source solutions are critical to support program transitions.

The Government will assess performer progress against target goals set for each phase using a progression of technical use case challenges as outlined below. In addition, an advisory panel composed of participants from Government partners may participate in the meetings and informal challenges to provide feedback to the DARPA Program Manager.

Technological Use Cases

HARDEN's TAs will address the following technological use cases of integrated software systems:

> (1) Unified Extended Firmware Interface (UEFI), chain-of-trust, and trusted boot technologies that govern trusted boot processes and integrity of a modern computing system; and
> (2) Integration technologies for securely connecting a tablet User Interface (UI) system with a trusted computer, such as a mission computer.

Performers will need to support both use cases for all tasks except TA2. TA2 proposers may choose to address only one, or both, of the use cases. If the choice is to address both use cases in the same proposal—for example, due to identified technological synergies and availability of platform expertise for both use cases—the proposers should make the tasking and the costs for each case clearly separable, so that the Government may select only one use case for a partial award, as explained later in this BAA.

In both of these integrated software system use cases, persistent vulnerabilities are known to exist. Patterns of exploitation and incomplete mitigations of these vulnerabilities suggest a wealth of uncontrolled emergent behaviors and abstraction leaks creating EE engines that can be successfully exploited by attackers across implementations of different provenance and by different vendors. HARDEN theories, models, methods, and tools will radically improve trustworthiness of these use cases by acting across multiple layers of its design and implementation.

Strong proposals to all TAs should discuss proposed approaches in terms of concrete exemplar systems matching the above use cases, for which the source code and the build processes are available for the majority of the system. Strong proposals should also discuss approaches for dealing with opaque system components in both software and hardware, such as methods for validating available specifications against the actual hardware, combining automated inference and automated interface exploration and interrogation.

More information about these use cases is provided below under "Exemplary Evaluation and Transition Use Cases" within this section.

TA1 – Tooling for developers

TA1 performers will develop and combine novel approaches for scalable reasoning about behaviors of computing systems' units, layers, components, and subsystems, to support multi-level modeling of system state evolution and emergent behaviors of unprotected abstractions. To support such reasoning, TA1 will develop novel theories, models, metadata, instrumentation, and tools.

TA1 tools will receive use case-specific models developed by TA2 throughout the program and will support reasoning about these models at the scales and granularities necessary to harden the software technologies essential to the trustworthiness of integrated system use cases described under "Technological Use Cases" within Section I.B. TA1 is expected to inform TA2's multi-level modeling of the integrated system use cases by providing feedback on which kinds of models can be concretely reasoned about.

TA1 will integrate these approaches and tools with popular development environments to produce effective and intelligible warnings of EE for system designers and developers, and will help them protect intended abstractions and create effective mitigations of EE across layers. These tools will be evaluated through use by the TA4 performer.

In addition, TA1 will provide its tools to TA3, who will use them in white-box testing of the exemplar systems.

Strong proposals should present a cohesive theory of EE that:

> (1) Enables automated reasoning about EE that is algorithmically efficient and implementation agnostic;
> (2) Consistent with insights from the latest edge-of-the-art exploitation experience;
> (3) Capable of being developed and applied incrementally to improve trustworthiness of the use cases; and
> (4) Enables tractable reasoning at the scales of the integrated software use cases.

Quantitative arguments that support the rationale for anticipated success of the proposed methods would strengthen proposals.

TA1 performers may employ any methods including, but not limited to, AI methods for searching large state spaces of EE models; hybrid, compiler-assisted analyses that leverage higher-level abstractions available at compilation; parametrized unit harnesses for testing expected behavior and automatic exploration of EE; interactive counterexample-guided methods; or any hybrid method. TA1 may complement static methods of analysis and EE disruption with dynamic methods, so long as the static and dynamic methods provide strong and cohesive assurance guarantees.

Developers working with the TA1 integrated environment will receive timely, interactive, and intelligible feedback on the propensity of their designs and implementations to create EE behaviors and will receive interactive guidance from the automated tools on how to mitigate it.

The TA1 integrated environment will take advantage of the existing specification, if any, interface control documents, if any, source code and related metadata, build chain, unit tests, and other information available for the use case code base, subject to the caveats under "Technological Use Cases" within Section I.B.

A TA1 capability will require research breakthroughs in overcoming state explosion of typical models of software behavior, making annotation of expected behavior and predictions of emergent behavior accessible to regular software developers, developing efficient means of communicating EE to developers, and integrating the ability to anticipate EE with common developer workflows and tools.

Strong TA1 proposals should discuss how the proposed effort will progress from basic models of the exemplar systems to increasing coverage and assurance of these systems. The Government would prefer that this progression is discussed in the context of concrete open-source software (or open software/hardware combination) that is representative of industry deployments and is relevant to the core technological use cases' trustworthiness. The discussion should clearly and quantitatively identify the challenges and obstacles on achieving superior security outcomes and present a compelling rationale for why the proposed approach will be successful at the scales and granularities necessary for large-scale commercial or open-source software development.

Proposals should present additional metrics and milestones for evaluating the progress of the envisioned approaches in the context of the discussed use case, in line with the general program metrics described below in Table 1.

Strong TA1 proposals will present a review of the existing approaches, techniques, and challenges, emphasizing industry experience, and applications to large integrated systems supported by appropriate literature citations.

Strong proposals will offer metrics and benchmarks for evaluating the success of the newly developed technologies in comparison to existing approaches in open reproducible settings. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open-source regimes. See Section IV.B.2.i for more details on Intellectual Property.

TA2 – Modeling of emergent behaviors

TA2 performers will focus on creating the capability for platform experts to model EE behavior in the use cases described under "Technological Use Cases" within Section I.B. TA2 performers will develop modeling methods, languages, and tools for characterizing emergent execution at different abstraction levels; produce and represent tiered and scalable models suitable for fast TA1 feedback; and will create models of EE for all relevant interfaces in the integrated system use cases.

In particular, TA2 performers will formulate approaches for modeling emergent behaviors across multiple layers of abstraction in integrated systems, and will use their subject matter expertise with the use case platforms and technologies to develop use-case specific models of emergent behaviors.

TA2's models will inform TA1's instrumentation of the development toolchain for reasoning about emergent behaviors at all available layers of abstraction, from the compiled binary code through the compiler abstractions and intermediate representations, to the highest levels of architectural abstraction. TA2's use-case specific models will be ingested and reasoned by TA1 tools. TA2 performers will receive feedback from TA1 regarding the models' amenability to reasoning at scale, and will iterate on the design and content of these models to support scaling.

Strong proposals should present cohesive modeling approaches to produce models that:

(1) Capture relevant descriptions of emergent behaviors empirically known to be of importance to the use cases' trustworthiness;
(2) Can be effectively reconciled with actual software and hardware behaviors;
(3) Are suitable for automated reasoning to anticipate emergent behaviors at the use case software scale envisioned by the BAA, so that the resulting solver computations needed to process the model should be within reach, possibly assuming some algorithmic breakthroughs;
(4) Can be formulated incrementally for the integrated system use cases; and
(5) Reflect expert-level knowledge of the use cases platforms and exploitation thereof.

Quantitative arguments to support the rationale for anticipated success of the proposed methods would strengthen proposals.

Strong TA2 proposals should address automation for deriving TA2 models from source code, build systems, or compiled binary code, and should seek to reduce the amount of platform subject matter expertise and labor needed to produce such models. TA2 modeling may take advantage of the existing specification (if any), interface control documents (if any), source code and related metadata, build chain, unit tests, and other information available for the use case code base, subject to the caveats under "Technological Use Cases" within this section.

Successful TA2 modeling approaches and tools are expected to be effective without complete knowledge of the implementations of underlying abstraction layers where such knowledge is not needed for anticipating adversarial programmability. Strong TA2 proposals should address the development of models for anticipating composability of emergent behaviors and for the reliable chaining of exploit primitives, even where the effects of any single behavior or flaw are reduced by current security mitigations.

Strong TA2 proposals will have detailed plans for supporting TA1's automated techniques for identifying implementations that are likely to result in composable emergent behaviors and for suggesting semantically equivalent implementation transformations that mitigate emergent composability and disrupt exploit programming. TA2 performers will be expected to work closely with TA3 and should provide a plan for interactions that leverage TA3's insights about state-of-the-art exploitation.

Strong proposals should discuss their modeling approaches and tools within the context of concrete open-source software (or an open software/hardware combination) that is representative of industry deployment and is relevant to the core technological use cases' trustworthiness. The discussion should clearly and quantitatively identify the challenges and obstacles to achieving superior security outcomes and present a compelling rationale for why the proposed approach will be successful at the scales and granularities necessary for large-scale commercial or open-source software development. Proposals should present metrics and milestones for evaluating the progress of the proposed approaches in the context of the discussed use cases, in line with the general program metrics described below in Table 1.

Strong TA2 proposals should present a review of the existing approaches, techniques, and challenges in academia and industry, supported by appropriate literature citations.

The program will emphasize creating and leveraging open-source technology and open-source architectures. Strong proposals are encouraged to offer metrics and benchmarks for evaluating the success of existing and newly developed technologies, in open reproducible settings. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open-source regimes to support broad transition. See Section IV.B.2.i for more details on Intellectual Property.

TA3 – Voice of the offense

The TA3 performer will focus on the generalization of edge-of-the-art exploitation patterns in close coordination with TA2 performers to help model EE and exploitation. The TA3 performer will identify and describe integrated system understanding and exploration techniques used in public exploitation of complex targets to locate composable primitives for multi-step exploitation methods.

The TA3 performer is expected to have or be able to procure strong subject-matter expertise in the technological stacks relevant to the use cases discussed in "Technological Use Cases" within Section I.B. Although the selection of specific technological exemplars of use case and transition platforms will be done by the TA4 performer, the TA3 performer will advise on the selection to ensure that these exemplars can be effectively hardened to prevent exploitation.

DARPA encourages TA3 proposers to address, at a minimum, the following topics:

(1) Explain the methodology for evaluating and selecting different architectural design choices for the HARDEN use cases in collaboration with the TA4 performer;
(2) Describe how the exemplar architectures will address potential partial deployment of HARDEN technologies across integrated systems (e.g., only some systems incorporate HARDEN functionality);
(3) Explore various options relating to the security of the HARDEN architecture itself, especially with respect to resistance to tampering by compromised devices and leakage via the TA1/TA2 mechanisms; and
(4) Integrate a system containing devices that represent a variety of platforms, operating systems, and application environments. Proposers should discuss the coordination of different TA1/TA2 mechanisms that operate across the various layers in the software stack and across different devices in the integrated system.

TA3 proposals should provide additional metrics to show increased efficiency of security analyses of targeted use case systems with TA1 tools and TA2 models over representative state-of-the-art red teaming methods. Strong TA3 proposals should also describe methods for developing tactics, techniques, and procedures capable of demonstrating specific weaknesses in the anticipated classes of TA1 and TA2 performers' hardening and assurance technologies, and integrated system software security analyses and assurance evidence.

The TA3 performer will assist the Government team in the development of evaluations for the technological capabilities developed by the TA1, TA2, and TA4 performers, and will provide feedback to the TA1, TA2, and TA4 performers. The TA3 performer will be responsible for defining and executing a pragmatic security testing approach that enables the incremental development, demonstration, evaluation, and eventual DoD transition of HARDEN capabilities. Strong TA3 proposals will provide open-source activity approaches that represent diverse, DoD-relevant use cases that support translating exploit development intuition and tradecraft into the formal modeling approaches of TA2.

The program will emphasize creating and leveraging open-source technology and open-source architectures. Strong proposals should offer metrics and benchmarks for evaluating the success

of the newly developed technologies in comparison to existing approaches in open, reproducible settings. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open-source regimes. See Section IV.B.2.i for more details on Intellectual Property.

TA4 – Integration and systems engineering evaluation

The TA4 performer will provide system integration and evaluation, applying tools developed by TA1 performers, and models developed by TA2 performers, to demonstrate reliable and effective hardening of a sensor system based on UEFI chain-of-trust ("trusted sensor") and of pilots' tablets and trusted mission system integration layer ("Cockpit tablet/User Interface (UI)").

TA4 proposals should initiate the application of concepts and techniques to critical system elements and high-assurance integrated military software systems with the goal of demonstrating the HARDEN capability of mitigating complex scenarios of exploitation, leveraging EE engines starting at early SDLC stages.

The TA4 performer will produce the testbed for demonstrating the HARDEN technological capabilities developed by TA1, TA2, and TA3 performers, and will evaluate these capabilities against the program metrics in coordination with the TA3 performer. The evaluation will include both security testing of the HARDEN technologies, and rigorous testing of the functional enhancements produced with these technologies via a series of evaluation/challenge exercises of increasing complexity and difficulty. The challenges should be suitable for fundamental research, shared without limitations with the TA1, TA2, and TA3 fundamental research teams, and should not contain Controlled Technical Information (CTI) or Controlled Unclassified Information (CUI).

TA4 proposals should also identify platforms and use cases for DoD transition, and apply tools and methodologies developed by the TA1 and TA2 performers to these use cases.

Strong TA4 proposals are encouraged to provide open-source approaches that support diverse technological use cases of software and hardware platforms relevant to the DoD.

The TA4 performer will provide the transition use cases and work with the DoD Services (Army, Navy, Air Force, and/or Marine Corps) to establish a HARDEN technology transition plan. The TA4 performer will also work with transition partner(s) for any transition accreditations or certifications required for transition of the resulting HARDEN capability to the services. The Government will require the TA4 performer to include personnel cleared, at a minimum, for SECRET level work with transition partner(s).

Evaluation Testbed Development

The series of evaluation/challenge exercises will progress in scale and complexity as detailed in Table 1, increasing the technical complexity of the challenges and the assurance guarantees that TA1 and TA2 technologies must meet.

In each evaluation/challenge exercise, TA1, TA2, and TA3 performers will receive source-level software/firmware or equivalent high-level representations of the code that will be their target to reason about EE and protect intended software abstractions from adversarial reuse. The TA1/TA2 performer evaluation code will be tested for desired functionality, robustness, and security.

Specific HARDEN end-of-program goals will be used during the Phase 3 evaluation/challenge assessment exercises. Strong proposals should present detailed plans for organizing the integrated hackathon demonstrations and evaluation/challenge exercises for the TA1, TA2, and TA3 performers using the TA4 testbed, as well as plans for allowing the performers suitable access to the testbed to prepare for these events.

Challenges should be drawn from the technologies relevant to the use cases discussed in "Technological Use Cases" within Section I.B, and work towards improved security outcomes in these integrated system use cases. The challenges should be suitable for fundamental research, should be shared without limitations with the TA1, TA2, and TA4 performers, and should not contain CTI or CUI.

Exemplary Evaluation and Transition Use Cases

The following discussion of an exemplary evaluation use case from the Air Force and Navy are provided below. Proposers are encouraged to enhance it with other relevant challenges, systems, and domains as needed to demonstrate safe and effective composition with the code base capabilities.

HARDEN will immediately address two multi-layer technologies important to the DoD:

> (1) The root-of-trust and supply chain trust management, such as the UEFI architecture and the DoD-specific Sensor Open System Architecture (SOSA); and
> (2) An architectural basis for a warfighter UI, such as pilots' tablets interfacing with the plane's mission computers.

The UEFI architecture was broadly adopted by industry to replace the legacy Basic Input/Output System (BIOS) and chipset firmware and provide a trustworthy architectural basis for root-of-trust and supply chain trust management. However, the UEFI ecosystem harbors rich classes of EE behaviors and offers a complex attack surface that permeates layers across the technology stack—from boot processes, to standalone drivers, to protected regions of memory and the main processor, to network connectivity—and cascades across the supply chain. HARDEN analyses and tools will disrupt the composability of EE behaviors at all layers of abstraction of the UEFI architecture to mitigate state-of-the-art threats and anticipate future threats.

SOSA is an Air Force Life Cycle Management Center (AFLCMC) initiative with broad industry engagement. SOSA's objective is to create standards for a variety of next generation DoD sensor systems. SOSA's key area of interest is the modeling and validation of the startup process of a sensor system to ensure system integrity before the sensor becomes operational. Complementary to SOSA's efforts, HARDEN will explore relevant firmware interfaces and events involved in a trusted computing system's startup, will help formulate standards to ensure system

trustworthiness, and will help create tools to validate compliance with these standards in SOSA systems.

The warfighter UI use case will explore secure integration of modern UI elements derived from Commercial Off-The-Shelf (COTS) technologies, such as pilots' tablets, with aircraft's mission systems and networks. Communications between pilots' tablets and the aircraft mission computers present a large attack surface inside and outside the aircraft. The HARDEN program will create state-of-the-art integrated systems analysis capabilities responsive to the assurance goals of trustworthy pilots' tablets.

If successful, HARDEN methodologies and tools will serve other types of DoD integrated systems, anticipating and pre-empting the root cause of exploitability in their design and implementation.

C. Program Phases and Metrics

The HARDEN program is a 48-month program organized into three phases: Phase 1 is an 18-month open-source component-scale phase, Phase 2 is an optional 18-month open-source subsystem-scale phase, and Phase 3 is an optional 12-month phase focused on scaling the technology to a DoD-relevant integrated system. The HARDEN technical and management milestones are depicted in Figure 2 below. As shown, program evaluation exercises are planned for months 9, 16, 23, 29, 35, 41, and 47. The month 9 evaluation will occur at the TA4 performer's facility and will be a TA1/TA2 integration hackathon demonstration. The integrator's testbed is to be established by month 9. The second program evaluation exercise at month 16 will be used to determine whether or not the performers should continue into Phase 2. Month 23 and 41 will also be TA1/TA2 integration hackathon demonstrations with the necessary testbed functionality improvements required for that phase to demonstrate program metrics in a realistic environment.

The capability milestones and metrics for the HARDEN program, shown in Table 1 below, are related to the capability to reason about EE and protect intended software abstractions from adversarial reuse. The specific metrics provided in the remainder of this section are indicative of the expected progress. Proposers should describe specific approaches that they will use for testing and evaluation purposes during each of the program phases, and propose additional quantitative metrics tailored to measuring progression of these approaches. Note that the platforms named in Table 1 for "Exemplary software complexity" are for gauging the approximate size and complexity of system under test, and not necessarily the actual use case exemplars.

	Metric	Phase I (18 mos)	Phase II (18 mos)	Phase III (12 mos)
All	Lines of Code, C/C++	50—100K	800K—1M	10—20M
	Exemplary software complexity	OpenWRT core IoT router/bridge firmware	TianoCore EDK2 UEFI firmware	Android (AOSP) subset/tablet ROS2/DDS avionics firmware (UAV)
TA1 & TA2	Instrumentation overhead	<=15%	<=10%	<=5%
	Time to transformation accuracy	1-2 months	<=4 weeks	<=4 days per component
	Coverage of objects and interfaces	60%, manual selection of test surface	80%, automated, with human-in-the-loop	95%, fully automatic test surface selection
	Alert / mitigation effectiveness	>=70% of tested emergent behaviors mitigated	>=80%	>=90%
TA3	Analysis efficiency over SoTA red team	10x on average	Up to 100x, 30—50x on average	1000x

Table 1: HARDEN Metrics

The Government will assess individual performer efforts in terms of the viability of their technical approaches, the trend in the performance of their systems over time, and their overall progress toward HARDEN program objectives.

Schedule and Milestones

For each year of effort, there will be quarterly meetings with the Program Manager (PM), consisting of two site visits and two Principal Investigator (PI) meetings. During these meetings/reviews, the PM will assess progress towards the solution via performer briefings, technical discussions, demonstrations, and informal end-of-phase evaluation/challenge exercises based on the target goals of each phase.

PI meetings will focus on open technical exchange. Difficulties encountered and possible solutions will also be discussed. The goals of the PI meetings will be to: (1) review and share innovations/accomplishments of the HARDEN program; (2) review and discuss plans and options for technology demonstrations and prototypes and HARDEN evaluation/challenge exercises; (3) review and discuss results from meetings and events conducted prior to and after the tests and evaluation/challenge exercises; (4) demonstrate prototypes; and (5) plan for the next six-month period.

The Government will specify the locations for the technical interchanges and PI meetings. Evaluation/challenge exercises will be held at the TA4 performer's site. For budgeting purposes, assume the locations of the two PI meetings held each year will alternate between Washington, D.C., and San Diego, CA. For budgeting travel to the TA4 performer's site, assume the location will be on the opposite coast from your location, or if regionally located in the Midwest, choose the more expensive coastal travel destination between San Diego, CA, or Washington, D.C. In addition to site visits, regular teleconference meetings are encouraged to enhance communications and collaborations, as required, among the performers. Should important issues arise between program reviews, the Government team will be available to support informal meetings. In-person meetings, evaluations, and site visits may be replaced with virtual ones if necessary.

Figure 2 below provides a tentative program schedule. Proposers should propose a detailed

schedule that is consistent with the maturity of their approaches and the risk reduction required for their concepts and their program plan. These schedules will be synchronized across performers, as required, and monitored and revised as necessary throughout the HARDEN program's period of performance. A start date of July 1, 2022, should be assumed for budgeting purposes.

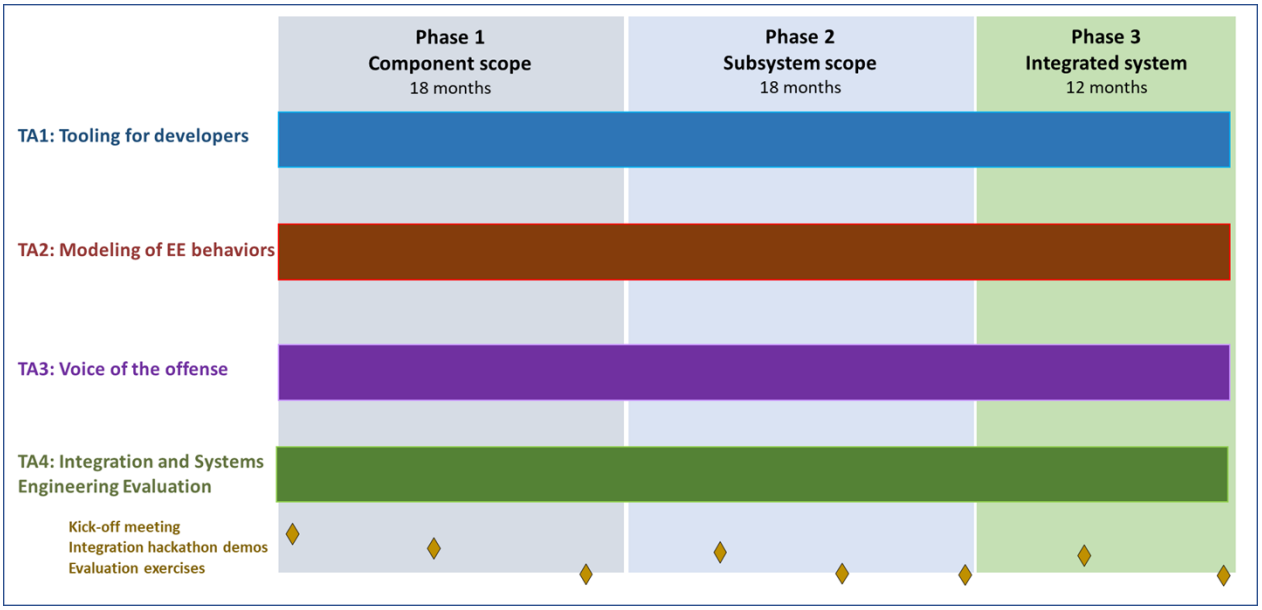

Figure 2: HARDEN Tentative Program Schedule

Deliverables

Performers are responsible for providing the following deliverables, as applicable:

- Slide Presentations – Annotated slide presentations will be submitted within two weeks after program kick-off meeting and after each review.
- Quarterly Coordination Reports – A quarterly technical coordination report describing progress made, resources expended, and any issues requiring the attention of the Government team will be provided within 10 calendar days after the end of each quarter.
- Monthly Financial Reporting – Monthly expenditure reports and uploading of required deliverables to the DARPA Vault reporting system are required by all HARDEN performers.
- System Development Plan (SDP) –The SDPs for each phase will be based on the performers' proposal and will be presented at the kickoff meeting for each phase. The SDP will describe the scope of the design and development effort, describe the hardware and software architecture in sufficient detail for review and planning, reference any applicable documents, and provide a program schedule. A SDP deliverable will be submitted within one month after the kickoff meeting for each phase, and shared with other performers for synchronization.
- Software – All computer software delivered under the HARDEN program must be delivered as source and object executable code. Include the source listings and source

code for the target computer systems, as well as any build scripts or other technical information required for the Government to compile all delivered source code. Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation.

- Software Documentation – Software documentation deliverables will be provided within one month after the end of each phase documenting source code, hardware description language specifications, system diagrams, part numbers, and other data necessary to maintain and to produce copies of the software.
- Hardware – At the conclusion of the period of performance, all hardware procured or developed under the HARDEN program will be delivered to the Government. The delivered components will be the same as those used to perform final performance tests and evaluations at the end of the period of performance. The delivery should include sufficient documentation to be completely operable, maintainable, and modifiable, with no reliance on any non-delivered hardware or hardware documentation developed or procured under the HARDEN program.
- Phased and Final Technical Reporting – End of phase reports are due at the conclusion of each phase, including through final phase contract completion. A separate Final Technical Report is due at the end of the period of performance. The reports will concisely summarize the effort conducted and provide any lessons learned during the development of the HARDEN technology.

All reporting must be delivered as required in Section VI.C.

D. Government-Furnished Property/Equipment/Information

Proposals should clearly state any assumptions regarding the use of proposed Government test facilities and capabilities, as well as any proposed Government-Furnished Equipment (GFE) used as part of their development, test, and evaluation approach. Proposers should not assume that the Government will provide them with any tools, hardware-in-the-loop testing tools, or ready-to-use threats needed to perform their tasks.

E. Intellectual Property

The program will emphasize creating and leveraging open-source technology and architecture. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open-source regimes. See Section IV.B.2.i for more details on Intellectual Property.

A key goal of the program is to establish an open, standards-based, multi-source, plug-and-play architecture that allows for interoperability and integration. This includes the ability to easily add, remove, substitute, and modify software and hardware components. This will facilitate rapid innovation by providing a base for future users or developers of program technologies and deliverables. Therefore, it is desired that all noncommercial software (including source code), software documentation, and technical data generated by the program be provided as deliverables to the Government with unlimited rights, and all hardware designs and documentation with a minimum of Government Purpose Rights (GPR), as lesser rights may

adversely impact the lifecycle costs of affected items, components, or processes.

II. Award Information

A. General Award Information

Multiple awards are anticipated under this BAA. The amount of resources made available under this BAA will depend on the quality of the proposals received and the availability of funds.

The Government reserves the right to select for negotiation all, some, one, or none of the proposals received in response to this solicitation and to make awards without discussions with proposers. The Government also reserves the right to conduct discussions if it is later determined to be necessary. If warranted, portions of resulting awards may be segregated into pre-priced options. Additionally, DARPA reserves the right to accept proposals in their entirety or to select only portions of proposals for award. In the event that DARPA desires to award only portions of a proposal, negotiations may be opened with that proposer. The Government reserves the right to fund proposals in phases with options for continued work, as applicable.

The Government reserves the right to request any additional, necessary documentation once it makes the award instrument determination. Such additional information may include but is not limited to Representations and Certifications (see Section IV.B.2.d, "Representations and Certifications"). The Government reserves the right to remove proposers from award consideration should the parties fail to reach agreement on award terms, conditions, and/or cost/price within a reasonable time, and the proposer fails to timely provide requested additional information. Proposals identified for negotiation may result in a procurement contract, cooperative agreement, or Other Transaction, depending upon the nature of the work proposed, the required degree of interaction between parties, whether or not the research is classified as Fundamental Research, 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 solicitation 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.

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 solicitation, the Government expects that program goals as described herein may be met by proposed efforts for fundamental research and non-fundamental research. Some proposed research may present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Based on the anticipated type of proposer (e.g., university or industry) and the nature of the solicited work, the Government expects that some awards will include restrictions on the resultant research that will require the awardee to seek DARPA permission before publishing any information or results relative to the program.

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 determine whether the proposed research shall be considered fundamental and to select the award instrument type. Appropriate language will be included in resultant awards for non-fundamental research to prescribe publication requirements and other restrictions, as appropriate. This language 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 to be performed by a potential awardee is non-fundamental research, its proposed subawardee's effort may be fundamental research. It is also possible that the research performed by a potential awardee is fundamental research while its proposed subawardee's effort may be non-fundamental research. In all cases, it is the potential awardee's responsibility to explain in its proposal which proposed efforts are fundamental research and why the proposed efforts should be considered fundamental research.

III. Eligibility Information

A. Eligible Applicants

All responsible sources capable of satisfying the Government's needs may submit a proposal that shall be considered by DARPA.

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 solicitation 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, that (a) cites the specific authority establishing their eligibility to propose to Government solicitations and compete with industry, and (b) certifies the FFRDC's compliance with the associated FFRDC sponsor agreement's terms and conditions. These conditions are a requirement 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 and compete with industry. This information is required for Government Entities proposing to be awardees or subawardees.

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. Other Applicants

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 solicitation. 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 solicitation 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. Cost sharing is encouraged where there is a reasonable probability of a potential commercial application related to the proposed research and development effort.

For more information on potential cost sharing requirements for Other Transactions for Prototype, see http://www.darpa.mil/work-with-us/contract-management#OtherTransactions.

IV. Application and Submission Information

A. Address to Request Application Package

This announcement, any attachments, and any references to external websites herein constitute the total solicitation. If proposers cannot access the referenced material posted in the announcement found at www.darpa.mil, contact the BAA Coordinator listed herein.

B. Content and Form of Application Submission

All submissions, including abstracts and proposals must be written in English with type not smaller than 12 point font. Smaller font may be used for figures, tables, and charts. Copies of all documents submitted must be clearly labeled with the DARPA BAA number, proposer organization, and proposal title/proposal short title.

1. Proposals Format

All proposals must be in the format given below. The typical proposal should express a consolidated effort in support of one or more related technical concepts or ideas. Disjointed efforts should not be included into a single proposal. Proposals shall consist of two volumes: 1) Volume I, Technical and Management Proposal (composed of three [3] Sections), and 2) Volume II, Cost Proposal. The maximum page count for Volume 1, Technical and Management Proposal, is 30 pages, and no more than 40 pages overall for proposals addressing multiple TAs, 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.

NOTE: Non-conforming submissions that do not follow the instructions herein may be rejected without further review.

Proposers may submit multiple proposals. In the case of submissions to multiple TAs or combinations of TAs as above, the Government reserves the right to decide which, if any, to select for award. A proposer submitting proposals to TA1 and TA2 may be selected to perform on one or both of these TAs. When submitting separate proposals for more than one TA, and selected for more than one TA, significant cost reductions for the combined effort will be expected, through synergies of the proposed approaches. However, TA3 and TA4 performers cannot perform on any other TA, to protect the integrity of the program evaluation and, in particular, of evaluating overall security improvements made to the use cases.

a) Volume I, Technical and Management Proposal

(1) Section I: Administrative

(a) Cover Sheet to Include

(1) BAA number (HR001121S0040)
(2) Technical area(s);
(3) Lead Organization submitting proposal;
(4) Type of organization, selected among the following categories: "LARGE BUSINESS", "SMALL DISADVANTAGED BUSINESS", "OTHER SMALL BUSINESS", "HBCU", "MI", "OTHER EDUCATIONAL", OR "OTHER NONPROFIT";
(5) Proposer's reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;
(8) Technical point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, electronic mail (if available);
(9) Administrative point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, electronic mail (if available);
(10) Total funds requested from DARPA, and the amount of cost share (if any); AND
(11) Date proposal was submitted.

(b) Official transmittal letter

(2) Section II: Summary of Proposal

A. Technical rationale, technical approach, and constructive plan for accomplishment of technical goals in support of innovative claims and deliverable creation.
B. Innovative claims for the proposed research. This section is the centerpiece of the proposal and should succinctly describe the uniqueness and benefits of the proposed approach relative to the current state-of-art alternate approaches.
C. Deliverables associated with the proposed research and the plans and capability to accomplish technology transition and commercialization. Include in this section all proprietary claims to the results, prototypes, intellectual property, or systems supporting and/or necessary for the use of the research, results, and/or prototype. If there are no proprietary claims, this should be stated. For forms to be completed regarding Intellectual Property, see Section IV.B.2.i of this BAA. There will be no page limit for the listed forms.
D. General discussion of other research in this area.
E. A clearly defined organization chart for the program team which includes, as applicable: (1) the programmatic relationship of team member; (2) the unique capabilities of team members;

(3) the task of responsibilities of team members; (4) the teaming strategy among the team members; and (5) the key personnel along with the amount of effort to be expended by each person during each year.

F. A summary slide of the proposed effort, in PowerPoint format, should be submitted with the proposal. Submit this PowerPoint file in addition to Volumes 1 and 2. The format for the summary slide is included as Appendix 1 to this BAA and does not count against the page limit.

(3) Section III: Detailed Proposal Information

A. Statement of Work (SOW) - Clearly define the technical tasks/subtasks to be performed, their durations, and dependencies among them. The page length for the SOW will be dependent on the amount of the effort. For each task/subtask, provide:
    - A general description of the objective (for each defined task/activity);
    - A detailed description of the approach to be taken to accomplish each defined task/activity;
    - Identification of the primary organization responsible for task execution (prime, sub, team member, by name, etc.);
    - The completion criteria for each task/activity - a product, event or milestone that defines its completion.
    - Define all deliverables (reporting, data, reports, software, etc.) to be provided to the Government in support of the proposed research tasks/activities; and
    - Clearly identify any tasks/subtasks (to be performed by either an awardee or subawardee) that will be accomplished on-campus at a university, if applicable.

Note: It is recommended that the SOW should be developed so that each Phase of the program is separately defined.

Do not include any proprietary information in the SOW.

B. Description of the results, products, transferable technology, and expected technology transfer path to supplement information included in the summary of the proposal. This should also address mitigation of life-cycle and sustainment risks associated with transitioning intellectual property for U.S. military applications, if applicable. Also see Section IV.B.2.i of this BAA, "Intellectual Property."
C. Detailed technical approach enhancing and completing that the Summary of Proposal.
D. Comparison with other ongoing research indicating advantages and disadvantages of the proposed effort.
E. Discussion of proposer's previous accomplishments and work in closely related research areas.
F. Description of Security Management architecture and/or approach for the proposed effort. Detail unique additional security requirements information system certification expertise for CUI or classified processing, Operation Security (OPSEC), program protection planning, test planning, transportation plans, work being performed at different classification levels, and/or utilizing test equipment not approved at appropriate classification level (may not be applicable for fundamental research).

G. Description of the facilities that would be used for the proposed effort (as applicable)
H. Detail support enhancing that of Summary of Proposal, including formal teaming agreements which are required to execute this program (as applicable)
I. Provide description of milestone, cost, and accomplishments.

b) Volume II, Cost Proposal

All proposers, including FFRDCs, must submit the following:

(1) Cover sheet to include:
(1) BAA number (HR001121S0040);
(2) Technical area(s);
(3) Lead Organization submitting proposal;
(4) Type of organization selected among the following categories: "LARGE BUSINESS", "SMALL DISADVANTAGED BUSINESS", "OTHER SMALL BUSINESS", "HBCU", "MI", "OTHER EDUCATIONAL", OR "OTHER NONPROFIT";
(5) Proposer's reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;
(8) Technical point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, electronic mail (if available);
(9) Administrative point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, and electronic mail (if available);
(10) Award instrument requested: cost-plus-fixed-fee (CPFF), cost-contract—no fee, cost sharing contract – no fee, or other type of procurement contract (specify), cooperative agreement, or Other Transaction;
(11) Place(s) and period(s) of performance;
(12) Total proposed cost separated by basic award and option(s) (if any);
(13) Name, address, and telephone number of the proposer's cognizant Defense Contract Management Agency (DCMA) or Office of Naval Research (ONR) administration office (if known);
(14) Name, address, and telephone number of the proposer's cognizant Defense Contract Audit Agency (DCAA) or comparable Educational Institutional audit office (if known);
(15) Date proposal was prepared;
(16) Data Universal Numbering System (DUNS) number;
(17) Taxpayer Identification Number (TIN);

(18) Commercial and Government Entity (CAGE) Code;
(19) Subawardee information; and
(20) Proposal validity period.

(2) Additional Cost Proposal Information

(a) Supporting Cost and Pricing Data

The proposer should include supporting cost and pricing information in sufficient detail to substantiate the summary cost estimates and should include a description of the method used to estimate costs and supporting documentation.

(b) Cost Breakdown Information and Format

Detailed cost breakdown to include:

- Total program costs broken down by major cost items (direct labor, including labor categories; subcontracts; materials; other direct costs; overhead charges, etc.) and further broken down by task and phase (Phase 1: 18-month Base, Phase 2: 18-month option, Phase 3: 12-month option; see cost spreadsheet details below).
- Major program tasks by fiscal year.
- An itemization of major subcontracts and equipment purchases.
- Documentation supporting the reasonableness of the proposed equipment costs (vendor quotes, past purchase orders/purchase history, detailed engineering estimates, etc.) shall be provided.
- An itemization of any information technology (IT) purchase, as defined by FAR 2.101 – Documentation supporting the reasonableness of the proposed equipment costs (vendor quotes, past purchase orders/purchase history, detailed engineering estimates, etc.) shall be provided, including a letter stating why the proposer cannot provide the requested resources from its own funding for prime and all sub-awardees.
- A summary of projected funding requirements by month.
- The source, nature, and amount of any industry cost-sharing.
- Identification of pricing assumptions of which may require incorporation into the resulting award instrument (e.g., use of Government Furnished Property/Facilities/Information, access to Government subject matter experts, etc.).

Tables included in the cost proposal in editable (e.g. MS Excel) format with calculation formulas intact. NOTE: If PDF submissions differ from the Excel submission, the PDF will take precedence.

The Government strongly encourages that proposers use the provided MS Excel™ DARPA Standard Cost Proposal Spreadsheet in the development of their cost proposals. A customized cost proposal spreadsheet may be an attachment to this solicitation. If not, the spreadsheet can be found on the DARPA website at http://www.darpa.mil/work-with-us/contract-management (under "Resources" on the right-hand side of the webpage). All tabs and tables in the cost proposal spreadsheet should be developed in an editable format with calculation formulas intact

to allow traceability of the cost proposal. This cost proposal spreadsheet should be used by the prime organization and all subcontractors. In addition to using the cost proposal spreadsheet, the cost proposal still must include all other items required in this announcement that are not covered by the editable spreadsheet. Subcontractor cost proposal spreadsheets may be submitted directly to the Government by the proposed subcontractor via e-mail to the address in Part I of this solicitation. **Using the provided cost proposal spreadsheet will assist the Government in a rapid analysis of your proposed costs and, if your proposal is selected for a potential award, speed up the negotiation and award execution process**.

Per FAR 15.403-4, certified cost or pricing data shall be required if the proposer is seeking a procurement contract award per the referenced threshold, unless the proposer requests and is granted an exception from the requirement to submit cost or pricing data. Certified cost or pricing data are not required if the proposer proposes an award instrument other than a procurement contract (e.g., a cooperative agreement, or other transaction).

(c) Subawardee Proposals

The awardee is responsible for compiling and providing all subawardee proposals for the Procuring Contracting Officer (PCO)/Grants Officer (GO)/Agreements Officer (AO), as applicable. Subawardee proposals should include Interdivisional Work Transfer Agreements (ITWA) or similar arrangements. Where the effort consists of multiple portions which could reasonably be partitioned for purposes of funding, these should be identified as options with separate cost estimates for each.

All proprietary subawardee proposal documentation, prepared at the same level of detail as that required of the awardee's proposal and which cannot be uploaded with the proposed awardee's proposal, shall be provided to the Government either by the awardee or by the subawardee organization when the proposal is submitted. In that case, subawardee proposals submitted to the Government by the proposed awardee or subawardee shall be submitted by email to HARDEN@darpa.mil. The subawardee must provide the same number of copies to the PCO/AO as is required of the awardee. See Section IV.B.2 of this BAA for proposal submission information.

(d) Other Transaction Requests

All proposers requesting an OT must include a detailed list of milestones. Each milestone must include the following:

- milestone description;
- completion criteria;
- due date; and
- payment/funding schedule (to include, if cost share is proposed, awardee and Government share amounts).

It is noted that, at a minimum, milestones should relate directly to accomplishment of program technical metrics as defined in the BAA and/or the proposer's proposal. Agreement type, expenditure or fixed-price based, will be subject to negotiation by the Agreements Officer. Do not include proprietary data.

2. Additional Proposal Information

a) Proprietary Markings

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 with a label such as "Proprietary"." NOTE: "Confidential" is a classification marking used to control the dissemination of U.S. Government National Security Information as dictated in Executive Order 13526 and should not be used to identify proprietary business information.

b) Security Information

(1) Program Security Information

Proposers should include with their proposal any proposed solution(s) to program security requirements unique to this program. Common program security requirements include but are not limited to: operational security (OPSEC) contracting/sub-contracting plans; foreign participation or materials utilization plans; program protection plans (which may entail the following) manufacturing and integration plans; range utilization and support plans (air, sea, land, space, and cyber); data dissemination plans; asset transportation plans; classified test activity plans; disaster recovery plans; classified material / asset disposition plans and public affairs/communications plans.

(2) CUI

At this time, this DARPA program does not anticipate issuing a DARPA HARDEN CUI guide. If there is a change in designation throughout the procurement process or performance of this DARPA program, a DARPA CUI guide will be provided at a later date through amendment of the BAA or modification to the awarded contract instrument. Identification of what is CUI about this DARPA program will be detailed in a DARPA CUI Guide and will be provided as an attachment to the BAA or may be provided at a later date.

(a) CUI Proposal Markings

If an unclassified submission contains CUI or the suspicion of such, as defined by Executive Order 13556 and 32 C.F.R. Part 2002, the information must be appropriately and conspicuously marked CUI in accordance with DoDI 5200.48.

(b) CUI Submission Requirements

Unclassified submissions containing CUI may be submitted via DARPA's BAA Website (https://baa.darpa.mil) in accordance with Section IV.B.2.b) of this BAA.

(c) Proposers submitting proposals involving the pursuit and protection of DARPA information designated as CUI must have, or be able to acquire prior to contract award, an information system authorized to process CUI information in accordance with (IAW) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and DoD Instruction (DoDI) 8582.01.

(3) Unclassified Submissions

DARPA anticipates that submissions received under this BAA will be unclassified. However, should a proposer wish to submit classified information, an unclassified email must be sent to the BAA mailbox requesting submission instructions from the Technical Office Program Security Officer (PSO). If a determination is made that the award instrument may result in access to classified information, a Security Classification Guide (SCG) and/or DD Form 254 will be issued by DARPA and attached as part of the award.

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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) and DoDI 8582.01 that are in effect at the time the solicitation 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.

d) Representations and Certifications

In accordance with FAR 4.1102 and 4.1201, proposers requesting a procurement contract must complete electronic annual representations and certifications at https://www.sam.gov/.

In addition, all proposers are required to submit for all award instrument types supplementary DARPA-specific representations and certifications at the time of proposal submission. See http://www.darpa.mil/work-with-us/reps-certs for further information on required representation and certification depending on your requested award instrument.

e) Human Subjects Research (HSR)/Animal Use

Proposers that anticipate involving human subjects or animals in the proposed research must comply with the approval procedures detailed at http://www.darpa.mil/work-with-us/additional-baa, to include providing the information specified therein as required for proposal submission.

f) Approved Cost Accounting System Documentation

Proposers that do not have a Cost Accounting Standards (CAS) complaint accounting system considered adequate for determining accurate costs that are negotiating a cost- type procurement contract must complete a Standard For, (SF 1408). For more information on CAS compliance, see http://www.dcaa.mil. 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.

g) Small Business Subcontracting Plan

Pursuant to Section 8(d) of the Small Business Act (15 U.S.C. § 637(d)) and FAR 19.702(a)(1), each proposer who submits a proposal for a procurement contract and includes subcontractors might be required to submit a subcontracting plan with their proposal. The plan format is outlined in FAR 19.704.

h) Section 508 of the Rehabilitation Act (29 U.S.C. § 749d)/FAR 39.2

All electronic and information technology acquired or created through this BAA must satisfy the accessibility requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 749d)/FAR 39.2.

i) Intellectual Property

All proposers must provide a good faith representation that the proposer either owns or possesses the appropriate licensing rights to all intellectual property that will be utilized under the proposed effort.

(1) For Procurement Contracts

Proposers responding to this BAA requesting procurement contracts will need to complete the certifications at Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7017. See http://www.darpa.mil/work-with-us/additional-baa for further information. If no restrictions are intended, the proposer should state "none." The table below captures the requested information:

Technical Data 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)

(2) For All Non-Procurement Contracts

Proposers responding to this BAA requesting a Cooperative Agreement, or Other Transaction shall follow the applicable rules and regulations governing these various award instruments, but, in all cases, should appropriately identify any potential restrictions on the Government's use of any Intellectual Property contemplated under the award instrument in question. This includes

both Noncommercial Items and Commercial Items. Proposers are encouraged use a format similar to that described in Paragraph (1) above. If no restrictions are intended, then the proposer should state "NONE."

j) 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 solicitation. 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/sys_attachment.do?sys_id=c08b64ab1b4434109ac5ddb6bc4bcbb8.

2. Submission Information

DARPA will acknowledge receipt of all submissions and assign an identifying control number that should be used in all further correspondence regarding the submission. DARPA intends to use electronic mail correspondence regarding HR001121S0040. Submissions may not be submitted by fax or e-mail; any submission received through fax or e-mail will be disregarded.

Submissions will not be returned. An electronic copy of each submission received will be retained at DARPA and all other non-required copies destroyed. A certification of destruction may be requested, provided the formal request is received by DARPA within five (5) business days after notification that a proposal was not selected.

For proposal submission dates, see Part I., Overview Information. Submissions received after these dates and times may not be reviewed.

The proposal must be received via DARPA's BAA Website (https://baa.darpa.mil) on or before, November 4, 2021, 12:00 noon, Eastern Time, in order to be considered during the initial round of selections; however, proposals received after this deadline may be received and evaluated up to solicitation closing of March 21, 2022, at 5:00 pm Eastern Time. Proposals submitted after the due date specified in the BAA or due date otherwise specified by DARPA may be selected. Proposers are warned that the likelihood of available funding is greatly reduced for proposals submitted after the initial closing date deadline.

a) Proposal Submission

Refer to Section VI.A.1. for how DARPA will notify proposers as to whether or not their proposal has been selected for potential award.

(1) For Proposers Requesting Cooperative Agreements

Proposers requesting 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 (DARPA-preferred); 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: In addition to the volumes and corresponding attachments requested elsewhere in this solicitation, proposers must also submit the three forms listed below.

Form 1: 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. § 1681 et.seq.), the Department of Defense (DoD) is collecting 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. In addition, the National Defense Authorization Act (NDAA) for FY 2019, Section 1286, directs the Secretary of Defense to protect intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security and limit undue influence, including foreign talent programs by countries that desire to exploit United States' technology within the DoD research, science and technology, and innovation enterprise. This requirement is necessary for all research and research-related educational activities. The DoD is using the two forms below to collect the necessary information to satisfy these requirements. Detailed instructions for each form are available on Grants.gov.

Form 2: 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.*

The Research and Related Senior/Key Person Profile (Expanded) form will be used to collect the following information for all senior/key personnel, including Project Director/Principal Investigator and Co-Project Director/Co-Principal Investigator, whether or not the individuals' efforts under the project are funded by the DoD:

- Degree Type and Degree Year.
- Current and Pending Support, including:
    - A list of all current projects the individual is working on, in addition to any future support the individual has applied to receive, regardless of the source.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other projects.

- The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.

- Name and address of the agencies and/or other parties supporting the other research projects

- Period of performance for the other research projects.

Additional senior/key persons can be added by selecting the "Next Person" button at the bottom of the form. Note that, although applications without this information completed may pass Grants.gov edit checks, if DARPA receives an application without the required information, DARPA may determine that the application is incomplete and may cause your submission to be rejected and eliminated from further review and consideration under the solicitation. DARPA reserves the right to request further details from the applicant before making a final determination on funding the effort.

Form 3: 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.*

(1) Grants.gov Submissions: Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. First time registration can take between three business days and four weeks. For more information about registering for Grants.gov, see http://www.darpa.mil/work-with-us/additional-baa.

(2) Hard-copy Submissions: Proposers electing to submit grant or cooperative agreement proposals as hard copies must complete the same forms as indicated above.

(2) For Proposers Requesting Technology Investment Agreements

Proposers requesting Technology Investment Agreements (TIA) awarded under 10 U.S.C. 2371 must include the completed form indicated below. This requirement only applies only to those who expect to receive a TIA as their ultimate award instrument.

The National Defense Authorization Act (NDAA) for FY 2019, Section 1286, directs the Secretary of Defense to protect intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security and limit undue influence, including foreign talent programs by countries that desire to exploit United States' technology within the DoD research, science and technology, and innovation enterprise. This requirement is necessary for all research and research-related educational activities. The DoD is using the form below to collect the necessary information to satisfy these requirements.

The Research and Related Senior/Key Person Profile (Expanded) form, available on the Grants.gov website at

https://apply07.grants.gov/apply/forms/sample/RR_KeyPersonExpanded_2_0-V2.0.pdf, will be used to collect the following information for all senior/key personnel, including Project Director/Principal Investigator and Co-Project Director/Co-Principal Investigator, whether or not the individuals' efforts under the project are funded by the DoD:

- Degree Type and Degree Year.
- Current and Pending Support, including:
    - A list of all current projects the individual is working on, in addition to any future support the individual has applied to receive, regardless of the source.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other projects.
    - The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.
    - Name and address of the agencies and/or other parties supporting the other research projects
    - Period of performance for the other research projects.

Additional senior/key persons can be added by selecting the "Next Person" button at the bottom of the form. Note that, although applications without this information completed may pass Grants.gov edit checks, if DARPA receives an application without the required information, DARPA may determine that the application is incomplete and may cause your submission to be rejected and eliminated from further review and consideration under the solicitation. DARPA reserves the right to request further details from the applicant before making a final determination on funding the effort.

(3) For Proposers Requesting Procurement Contracts or OTs and Submitting to a DARPA-approved Proposal Submissions Website

Unclassified full proposals sent in response to this BAA shall be submitted via DARPA's BAA Website (https://baa.darpa.mil). Note: If an account has already been created for the DARPA BAA Website, this account may be reused. If no account currently exists for the DARPA BAA Website, visit the website to complete the two-step registration process. Submitters will need to register for an Extranet account (via the form at the URL listed above) and wait for two separate e-mails containing a username and temporary password. After accessing the Extranet, submitters may then create an account for the DARPA BAA website (via the "Register your Organization" link along the left side of the homepage), view submission instructions, and upload/finalize the proposal. Proposers using the DARPA BAA Website may encounter heavy traffic on the submission deadline date; proposers should start this process as early as possible.

All unclassified concepts submitted electronically through DARPA's BAA Website must be uploaded as zip files (.zip or .zipx extension). The final zip file should be no greater than 50 MB in size. Only one zip file will be accepted per submission, and submissions not uploaded as zip files will be rejected by DARPA.

Classified submissions and proposals requesting grants or cooperative agreements should NOT be submitted through DARPA's BAA Website (https://baa.darpa.mil), though proposers will likely still need to visit https://baa.darpa.mil to register their organization (or verify an existing registration) to ensure the BAA office can verify and finalize their submission.

Technical support for DARPA's BAA Website may be reached at BAAT_Support@darpa.mil, and is typically available during regular business hours, Eastern Time.

3. Frequently Asked Questions (FAQ)

DARPA will post a consolidated Frequently Asked Questions (FAQ) document. To access the posting go to: http://www.darpa.mil/work-with-us/opportunities. Under the HR001121S0040 summary will be a link to the FAQ. Submit your questions by E-mail to HARDEN@darpa.mil. Questions must be received by the FAQ/Questions due date listed in Part I, Overview Information.

V. Application Review Information

A. Evaluation Criteria

Proposals will be evaluated using the following criteria, listed in descending order of importance:

1. Overall Scientific and Technical Merit

The proposed technical approach is innovative, feasible, achievable, and complete.

The proposed technical team has the expertise and experience to accomplish the proposed tasks. Task descriptions and associated technical elements provided are complete and in a logical sequence with all proposed deliverables clearly defined such that a final outcome that achieves the goal can be expected as a result of award. The proposal identifies major technical risks and planned mitigation efforts are clearly defined and feasible.

The proposal clearly explains the technical approach(es) that will be employed to meet or exceed each program goal and metric listed in Section I.C and provides ample justification as to why the approach(es) is feasible. The Government will also consider the structure, clarity, and responsiveness to the Statement of Work; the quality of proposed deliverables; and the linkage of the Statement of Work, technical approach(es), risk mitigation plans, costs, and deliverables of the prime awardee and all subawardees through a logical, well structured, and traceable technical plan.

2. 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.

3. Cost and Schedule 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).

It is expected that the effort will leverage all available relevant prior research in order to obtain the maximum benefit from the available funding. For efforts with a likelihood of commercial application, appropriate direct cost sharing may be a positive factor in the evaluation. DARPA recognizes that undue emphasis on cost may motivate proposers to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel in order to be in a more competitive posture. DARPA discourages such cost strategies.

The proposed schedule aggressively pursues performance metrics in an efficient time frame that accurately accounts for the anticipated workload. The proposed schedule identifies and mitigates any potential schedule risk.

B. Review of Proposals

1. Review Process

It is the policy of DARPA to ensure impartial, equitable, comprehensive proposal evaluations based on the evaluation criteria listed in Section V.A and to select the source (or sources) whose offer meets the Government's technical, policy, and programmatic goals.

DARPA will conduct a scientific/technical review of each conforming proposal. Conforming proposals comply with all requirements detailed in this solicitation; 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.

Award(s) will be made to proposers whose proposals are determined to be the most advantageous to the Government, consistent with instructions and evaluation criteria specified in the BAA herein, and availability of funding.

2. Handling of Source Selection Information

DARPA policy is to treat all submissions as source selection information (see FAR 2.101 and 3.104), and to disclose their contents only for the purpose of evaluation. Restrictive notices notwithstanding, during the evaluation process, submissions may be handled by support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors performing this role are expressly prohibited from performing DARPA-sponsored technical research and are bound by appropriate nondisclosure agreements. 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.

3. Federal Awardee Performance and Integrity Information (FAPIIS)

Per 41 U.S.C. § 2313, as implemented by FAR 9.103 and 2 C.F.R. § 200.205, prior to making an award above the simplified acquisition threshold, DARPA is required to review and consider any information available through the designated integrity and performance system (currently FAPIIS). Awardees have the opportunity to comment on any information about themselves entered in the database, and DARPA will consider any comments, along with other information in FAPIIS or other systems prior to making an award.

VI. Award Administration Information

A. Selection Notices and Notifications

Proposals

As soon as the evaluation of a proposal is complete, the proposer will be notified that (1) the proposal has been selected for funding pending award negotiations, in whole or in part, or (2) the proposal has not been selected. These official notifications will be sent via email to the Technical Point of Contact (POC) and/or Administrative POC identified on the proposal coversheet.

B. Administrative and National Policy Requirements

1. Solicitation Provisions and Award Clauses, Terms and Conditions

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 http://www.darpa.mil/work-with-us/additional-baa.

2. Controlled Unclassified Information (CUI) and Controlled Technical Information (CTI) on Non-DoD Information Systems

Further information on Controlled Unclassified Information identification, marking, protecting, and control, to include processing on Non-DoD Information Systems, is incorporated herein and can be found at http://www.darpa.mil/work-with-us/additional-baa.

3. Terms and Conditions

For terms and conditions specific to grants and/or cooperative agreements, see the DoD General Research Terms and Conditions (latest version) at http://www.onr.navy.mil/Contracts-Grants/submit-proposal/grants-proposal/grants-terms-conditions and the supplemental DARPA-specific terms and conditions at http://www.darpa.mil/work-with-us/contract-management#GrantsCooperativeAgreements.

C. Reporting

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

D. Electronic Systems

1. Wide Area Work Flow (WAWF)

Performers will be required to submit invoices for payment directly to https://piee.eb.mil/, unless an exception applies. Performers must register in WAWF prior to any award under this BAA.

2. i-Edison

The award document for each proposal selected for funding will contain a mandatory requirement for patent reports and notifications to be submitted electronically through i-Edison (https://public.era.nih.gov/iedison).

E. DARPA Embedded Entrepreneur Initiative (EEI)

Awardees pursuant to this solicitation may be eligible to participate in the DARPA Embedded Entrepreneurship Initiative (EEI) during the award's period of performance. EEI is a limited scope program offered by DARPA, at DARPA's discretion, to a small subset of awardees. The goal of DARPA's EEI is to increase the likelihood that DARPA-funded technologies take root in the U.S. and provide new capabilities for national defense. EEI supports DARPA's mission "to make pivotal investments in breakthrough technologies and capabilities for national security" by accelerating the transition of innovations out of the lab and into new capabilities for the Department of Defense (DoD). EEI investment supports development of a robust and deliberate Go-to-Market strategy for selling technology product to the government and commercial markets

and positions DARPA awardees to attract U.S. investment. The following is for informational and planning purposes only and does not constitute solicitation of proposals to the EEI.

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

EEI Application Process:
After receiving an award under the solicitation, awardees interested in being considered for EEI should notify their DARPA Program Manager (PM) during the period of performance. Timing of such notification should ideally allow sufficient time for DARPA and the awardee to review the awardee's initial transition plan, identify milestones to achieve under EEI, modify the award, and conduct the work required to achieve such milestones within the original award period of performance. These steps may take 18-24 months to complete, depending on the technology. If the DARPA PM determines that EEI could be of benefit to transition the technology to product(s) the Government needs, the PM will refer the performer to DARPA Commercial Strategy.

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

Invitation to participate in EEI is at the sole discretion of DARPA and subject to program balance and the availability of funding. EEI participants' awards may be subsequently modified bilaterally to amend the Statement of Work to add negotiated EEI tasks, provide funding, and specify a milestone schedule which will include measurable steps necessary to build, refine, and

execute a Go-to-Market strategy aimed at delivering new capabilities for national defense. Milestone examples are available at: https://www.darpa.mil/work-with-us/contract-management

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

VII. Agency Contacts

Administrative, technical, or contractual questions should be sent via email to HARDEN@darpa.mil. All requests must include the name, email address, and phone number of a point of contact.

Points of Contact
The BAA Coordinator for this effort may be reached at HARDEN@darpa.mil.
The Technical POC for this effort is Sergey Bratus.
DARPA/I2O
ATTN: HR001121S0040
675 North Randolph Street
Arlington, VA 22203-2114

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

VIII. Other Information

Proposers Day

A virtual Proposers Day for this effort will be held on September 30, 2021.
The Special Notice regarding this Proposers Day can be found at:
https://www.schafertmd.com/darpa/i2o/HARDEN/pd/

For further information regarding the HARDEN Proposers Day, including slides from the event, please see http://www.darpa.mil/work-with-us/opportunities under HR001121S0040.

Associate Contractor Agreement (ACA)

This same or similar language will be included in procurement contract awards against HR001121S0040. Awards other than FAR based contracts will contain similar agreement language:

(a) It is recognized that success of the HARDEN research effort depends in part upon the open exchange of information between the various Associate Contractors involved in the effort. This language is intended to ensure that there will be appropriate coordination and integration of work by the Associate Contractors to achieve complete compatibility and to prevent unnecessary duplication of effort. By executing this contract, the Contractor assumes the responsibilities of an

Associate Contractor. For the purpose of this ACA, the term Contractor includes subsidiaries, affiliates, and organizations under the control of the contractor (e.g., subcontractors).

(b) Work under this contract may involve access to proprietary or confidential data from an Associate Contractor. To the extent that such data is received by the Contractor from any Associate Contractor for the performance of this contract, the Contractor hereby agrees that any proprietary information received shall remain the property of the Associate Contractor and shall be used solely for the purpose of the HARDEN research effort. Only that information which is received from another contractor in writing and which is clearly identified as proprietary or confidential shall be protected in accordance with this provision. The obligation to retain such information in confidence will be satisfied if the Contractor receiving such information utilizes the same controls as it employs to avoid disclosure, publication, or dissemination of its own proprietary information. The receiving Contractor agrees to hold such information in confidence as provided herein so long as such information is of a proprietary/confidential or limited rights nature.

(c) The Contractor hereby agrees to closely cooperate as an Associate Contractor with the other Associate Contractors on this research effort. This involves as a minimum:

(1) maintenance of a close liaison and working relationship;

(2) maintenance of a free and open information network with all Government-identified associate Contractors;

(3) delineation of detailed interface responsibilities;

(4) entering into a written agreement with the other Associate Contractors setting forth the substance and procedures relating to the foregoing, and promptly providing the Agreements Officer/Procuring Contracting Officer with a copy of same; and,

(5) receipt of proprietary information from the Associate Contractor and transmittal of Contractor proprietary information to the Associate Contractors subject to any applicable proprietary information exchange agreements between associate contractors when, in either case, those actions are necessary for the performance of either.

(d) In the event that the Contractor and the Associate Contractor are unable to agree upon any such interface matter of substance, or if the technical data identified is not provided as scheduled, the Contractor shall promptly notify the DARPA HARDEN Program Manager. The Government will determine the appropriate corrective action and will issue guidance to the affected Contractor.

(e) The Contractor agrees to insert in all subcontracts hereunder which require access to proprietary information belonging to the Associate Contractor, a provision which shall conform substantially to the language of this ACA, including this paragraph (e).

(f) Associate Contractors for the HARDEN research effort include:

Contractor	Technical Area

IX. APPENDIX 1 – PROPOSAL SUMMARY SLIDE

FP: Prime Organization Name
PI: PI Name (%LOE)
Subcontractors: Subcontractors
Title: proposal title

TA#

HARDEN

Summary:

- Succinctly describe the proposed technical approach (be sure to convey key insights)
- The bullets, combined with the graphic below, should clearly convey what is proposed
- Use the bullets as the "elevator speech" for the proposal
- Etc. (use as many bullets as necessary)

Insert high-resolution overview graphic of proposed architecture/technical approach from proposal

Source: Prime Organization, Volume 1 (HARDEN)

Innovation, feasibility:

- High-level bullets for how the approach is particularly innovative (i.e., goes beyond current state-state-of-the-art)
- Why the approach is feasible (at a high-level)
- Etc. (use as many bullets as necessary)

Risks/mitigations:

- Identification of high-risk elements (e.g., limitations) of your approach
- High-level description of risk(s) mitigation
- Etc. (use as many bullets as necessary)

Cost:

- Prime $s and % of overall cost (e.g., ABC Inc.: $#.#M, X%)

Intellectual Property/data rights assertions:

- Yes/No (with very brief description if warranted)

Human Subjects Research:

- Brief description of HSR, if proposed (or 'No'). Note that crowd-sourcing should be listed if proposed.

Summary	Phase 1	Phase 2	Phase 3	Total
Proposed	$#.#M	$#.#M	$#.#M	$#.#M

Submit as an MS PowerPoint Chart. Do not change font (Tahoma). Convert all red text to black text upon submission. Do not alter existing black text. 1