Broad Agency Announcement

Safe Documents (SafeDocs)

HR001118S0054

August 23, 2018

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

Table of Contents

PART I: OVERVIEW INFORMATION

- **Federal Agency Name:** Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)

- **Funding Opportunity Title:** Safe Documents (SafeDocs)

- **Announcement Type:** Initial Announcement

- **Funding Opportunity Number:** HR001118S0054

- **Catalog of Federal Domestic Assistance Numbers (CFDA):** 12.910 Research and Technology Development

- **Dates**
  - Posting Date: August 23, 2018
  - Proposers Day: August 24, 2018
  - Abstract Due Date: September 7, 2018, 12:00 noon (ET)
  - Proposal Due Date: October 19, 2018, 12:00 noon (ET)
  - BAA Closing Date: October 19, 2018, 12:00 noon (ET)

- **Anticipated Individual Awards:** DARPA anticipates multiple awards for technical areas 1 and 2; and single awards for technical areas 3 and 4.

- **Types of Instruments that May be Awarded:** Procurement contracts, cooperative agreements or Other Transactions (grants will not be awarded)

- **Agency Contacts**

  - **Technical POC**: Dr. Sergey Bratus, Program Manager, DARPA/I2O

  - **BAA Email**: SafeDocs@darpa.mil

  - **BAA Mailing Address**:

    DARPA/I2O
    ATTN: HR001118S0054
    675 North Randolph Street
    Arlington, VA 22203-2114

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

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

DARPA is soliciting innovative research proposals in the area of secure processing of untrusted electronic data. Proposed research should investigate innovative approaches that radically improve software's ability to recognize and safely reject invalid and maliciously crafted input data, while preserving essential functionality of legacy electronic data formats. Proposals should build on an existing base of knowledge of electronic document, message, and streaming formats and the nature of security vulnerabilities associated with these formats.

DARPA is interested in innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

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

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

The following information is for those wishing to respond to this BAA.

A. Background

Electronic documents are ubiquitous and essential to all aspects of modern life. Individuals and organizations must routinely engage with electronic documents received from a variety of unauthenticated or potentially compromised sources, comprising a growing variety of electronic data formats. Even if the immediate provider of the data can be authenticated, the data may derive from an untrusted source.

We expect pictures, charts, spreadsheets, maps, audio, video, as well as rich messages potentially including any and all of these, to be received with a click of a button. However, the complexity of managing such electronic data results in software vulnerable to attack. This situation is unsustainable.

Current software that processes electronic data such as documents, messages, and data streams is error-prone and vulnerable to exploitation by malicious inputs. According to MITRE's Common Vulnerability Enumeration data, over 80% of yearly reported vulnerabilities occur in code that handles input data. Such code converts a given bit stream representing the data into memory objects and validates that these objects have expected structure and relationships.

Exploitation of input-handling vulnerabilities leverages inaccurate programmer assumptions regarding the extent to which input data has been validated by input-handling code. Code that behaves correctly under certain assumptions (and may even be proven correct under these assumptions) will typically *not* behave correctly if any of these assumptions do not hold. Attackers can induce incorrect behaviors by presenting vulnerable software with maliciously crafted input data that violates unchecked assumptions. The programmer assumes that validated input data contains certain objects in certain relationships, and writes code under these assumptions. However, should any of these assumptions not hold, the code will not behave correctly. A single missing or incorrect check can create a vulnerability, as was the case with the Heartbleed vulnerability (CVE-2014-0160), in which code acting on an unchecked assumption exposed sensitive memory content to remote attackers.

Parsing or checking code itself contains exploitable flaws and behaviors. Such flaws are particularly insidious, as they require little or no human interaction for the attack to succeed or lead to pre-authentication vulnerabilities.

B. Insufficiency of Current Approaches

Today, code for input data validation is typically written manually in an ad-hoc manner. For commonly-used electronic data formats, input validation is, at a minimum, a problem of scale whereby specifications of these formats comprise hundreds to thousands of pages. Input validation thus translates to thousands or more conditions to be checked against the input data before the data can be safely processed. Manually writing the code to parse and validate input, and then manually auditing whether that code implements all the necessary checks completely and correctly, does not scale.

Moreover, manual parser coding and auditing typically fail even for electronic data formats specifically designed to be easier to perform such tasks, e.g., JSON and XML. A variety of critical vulnerabilities have been found in major parser implementations for these formats.

Widely deployed mitigations against crafted input attacks include (a) trying to prevent the flow of untrusted data to vulnerable software; and (b) testing of software with randomized inputs to find and patch flaws that could be triggered by maliciously created inputs.

Unfortunately, neither of these approaches offers security assurance guarantees.

Mitigations for preventing the flow of untrusted data to vulnerable software, which can be implemented via network or host-based measures such as firewalls, application proxies, anti-virus scanners, etc., neither remove the underlying vulnerability from the target, nor encode complete knowledge of document or message format internals. Attacker bypasses of such mitigations exploit incompleteness of the mitigations' understanding of the data format to exploit the still-vulnerable targets.

The effectiveness of fuzzing methods for testing of software with randomized inputs to find and fix flaws depends on whether randomly generated inputs can emulate maliciously crafted inputs closely enough to trigger all relevant code flaws. Although modern fuzzing methods incorporate feedback from tracing the execution of the code as it consumes crafted inputs, they also employ symbolic and concolic execution of code in their exploration of the space of potential crafted inputs. As a result, these methods are still essentially heuristic. There is no guarantee that attackers, who also use fuzzing to locate and develop vulnerabilities, will not cover a more substantial and more productive portion of the input space with a different set of heuristics.

In contrast, approaches based on automatic generation and analysis of code (and, potentially, formal verification of such code to be functionally correct) offer security assurances. Such approaches produce code that is significantly less error-prone and vulnerable. Some of this code can even be automatically verified and proven to be correct, as was demonstrated, e.g., by the DARPA High-Assurance Cyber Military Systems (HACMS) program.

However, these approaches are typically not applied to code that parses and validates the dominant electronic data formats. Automatic code generation tools and code verification tools cannot function without a precise specification, which also must be of reasonable complexity to enable verification. Regrettably, the application of formal methods is impeded by the ambiguity and complexity of the formats.

Ambiguity: Even though electronic data formats such as Portable Document Format (PDF) have published specifications approved by standards bodies such as the International Organization for Standardization, dominant implementations of these formats extend the standards by deliberately accepting non-compliant inputs without any indication to the users that the document contains malformations silently presumed benign. Actual populations of electronic documents (referred to as *extant* in this BAA) contain many such malformations, which are not documented, but for all practical purposes have been allowed to become a part of the de facto format syntax. Being undocumented, these silent "fixing" behaviors have led to phenomena such as strikingly different interpretations of the same document or message by different implementations.

Complexity: Existing standards, even when fully complied with, do not seek to limit the syntactic complexity of the data. As a result, they allow constructs that, although never used in benign documents, make formal reasoning about code that would validate such constructs very hard or even undecidable.

C. Program Description/Scope

The Safe Documents (SafeDocs) program will develop novel verified programming methodologies for building high assurance parsers for extant electronic data formats, and novel methodologies for comprehending, simplifying, and reducing these formats to their safe, unambiguous, verification-friendly subsets ("safe sub-setting").

SafeDocs will address the ambiguity and complexity obstacles to the application of verified programming posed by extant electronic data formats. SafeDocs' multi-pronged approach will combine:

a) extraction of the extant formats' de facto syntax (including any non-compliant syntax deliberately accepted and substantially used in the wild);
b) identifying a syntactically simpler subset of this syntax that yields itself to use in verified programming while preserving the format's essential functionality; and
c) creating software construction kits for building secure, verified parsers for this syntactically simpler subset, and high-assurance translators for converting extant instances of the format to this subset.

The parser construction kits developed by SafeDocs will be usable by industry programmers who understand the syntax of electronic data formats but lack the theoretical background in verified programming. These tools will enable developers to construct verifiable parsers for new electronic data formats as well as extant ones. The tools will guide the syntactic design of new formats, by making verification-friendly format syntax easy to express, and vice versa.

SafeDocs will distinguish between electronic data formats for *documents* understood as static, self-contained content, and formats for *streaming* electronic data from external devices such as Internet of Things (IoT) endpoints or sensors. This distinction reflects two modes of parsing and validation for security purposes (discussed in more detail below in TA2). Documents can be examined as a whole, in an early phase of their processing, validated, judged as “safe” at that particular point in time, and remain “safe” from that point onwards. By contrast, streaming data requires continual low-latency validation of incoming data.

Electronic document formats are understood to contain formatted text, images, and allow a limited amount of user interaction, but do not include general-purpose executable functionality or continual external updates (compare common uses of PDF for electronic office workflows and archiving). Data streaming formats are understood to provide machine-to-machine real-time data exchanges such as, e.g., streams encapsulated by the Data Distribution Service (DDS), up to and including video and sound streams.

SafeDocs will focus on flaw-free processing of input syntax. Cryptography-based approaches are not in scope for the SafeDocs program. Parsing failures and syntactic ambiguities of cryptographic formats are a known source of weakness in implementations of cryptographic systems, exploited to bypass their theoretical guarantees. SafeDocs aims to protect cryptographic constructs along with other kinds of data objects.

The SafeDocs program consists of four Technical Areas (TAs):

- TA1: Extant Syntax Recovery, Simplification, and Safe Sub-setting.
- TA2: Constructing Secure Parsers
- TA3: Testing and Evaluation
- TA4: Instantiation

C.1 TA1: Extant Syntax Recovery, Simplification, and Safe Sub-setting

TA1 will develop methodology, formalism, and tools to capture and describe de facto syntax of electronic data formats in human-intelligible, machine-readable form, combining as sources of information the published specifications of the format, a large corpus of extant instances of the format (such as electronic documents or messages in the wild), and the binaries (or source code, where available) of existing dominant software implementations. This methodology will recover the ground truth of an extant electronic format, creating a basis on which the use and abuse of the format's features in the wild may be evaluated. In doing so, TA1 will produce the first effective metrics and comprehensive analysis of the format’s ambiguity in actual use.

TA1 will identify syntactic complexity obstacles that extant formats present to automated verification methods. TA1 will also develop methodologies and tools for the selection of a simpler ‘safe’ syntactic subset of a format that, while preserving the format's essential functionality, is free of these obstacles. TA1’s human-intelligible, machine-readable description of the format will be used by TA2 to build high-assurance and verifiable parsers for the format.

These goals will require breakthroughs in the theory and practice of automated comprehension of electronic data formats.

Outcomes of TA1

TA1 will produce an automated methodology for comprehending an extant data format, as described below, resulting in a machine-and-human-readable formal description of a simplified unambiguous subset ("*safe subset*") of the de facto format syntax that is suitable for defining and verifying:

a. a secure functionally correct parser for the data language, and
b. a high-assurance translator from the de facto syntax (including malformations presumed benign, allowed syntactic ambiguities, syntactic exuberances, and syntactic redundancies) to the simplified unambiguous subset of the format.

The automated methodology for comprehension of an extant electronic data format will draw upon its published standards, its dominant implementations, and a large (at least $10^6 – 10^9$ samples) corpus of its extant instances such as documents or messages (for evaluation purposes, TA3 will provide reference corpora for selected formats). This methodology will allow format subject matter experts to quickly review the "ground truth" of the de facto format syntax, and to make determinations of which features or malformations presumed benign can be allowed in the simplified format or can be converted to this format canonically and composably to yield the functionally correct translator as described above.

Strong proposals for TA1 will show capability to collect the data needed to recover the ground truth of extant electronic data formats and to identify security-relevant format phenomena (see the following section titled "Empirical Exploration of Extant Format Phenomena"), but should also plan to work with TA3 to refine their understanding of the extant formats' challenges.

TA1 Theory Challenges

Specifications of extant electronic data formats, with few exceptions, can be characterized as:

- ambiguous or imprecise (being written in natural language);
- not machine readable (similar but not quite the same as above);
- de facto redefined or extended by permissive implementations; and
- divergent (due to multiple, non-specified kinds of permissive handling of non-compliant data by implementations).

Syntactically, extant electronic data formats are sets of dialects that purport to have the same syntax and semantics, and agree on it in their large core part, but also diverge syntactically and semantically in ways that impact security.

Current theory lacks convenient abstractions for describing syntactic phenomena associated with extant electronic data formats. For example, existing formal language theory abstractions:

- do not describe the phenomena of divergent dialects of a language;
- do not offer the simplest notional description of the assumed syntactic properties of data;
- do not account for permissiveness and ambiguity effects; and

- do not provide a way to compositionally reason about transformations between syntactic expressions meant to be equivalent.

Formal devices currently used to capture data format syntax, e.g., Backus-Naur Form (BNF), Extended Backus-Naur Form (EBNF), etc., in such standards specifications that use them, share the above drawbacks.

Strong proposals will outline the current state of the art in regard to the challenges of describing extant electronic data formats, identify weaknesses of current approaches, and plan to address them with a comprehensive formal approach that enables reasoning about the format and its implementations.

The approach must enable creation of high-assurance parsers for the formats that exhibit phenomena such as diverging concepts of allowable syntactic malformation, divergent interpretations of syntactic validity and equivalence of syntactic constructs, as well as the existence of a core language on which multiple implementations agree.

The formalism will describe ways in which occurrences of equivalent syntactic expressions can be converted to a preferred simplest form, and provide means of reasoning about composing such local syntactic transforms. The formalism should not assume global syntactic consistency, i.e., that all such transforms are compatible or composable.

TA1 proposals that explore several competing or complementary formal approaches should describe each approach as a separate statement-of-work task and provide sufficient costing details for such tasks to be separable.

Empirical Exploration of Extant Format Phenomena

Strong TA1 proposals will recognize the need to explore empirical properties of extant data formats, such as syntactic features that often result in unintended execution (a.k.a. exploitation), the existence of “polyglot” files (files that simultaneously conform to several unrelated published standards or de facto format syntax at the same time) and the so-called “schizophrenic” files. Schizophrenic files fit several divergent de facto dialects of the same data format, and whose syntactic structure is interpreted differently in these dialects, and, as a result, are understood differently by different interpreters of the format. Strong proposals will maintain this awareness through all layers of syntax down to the bit-level data representation.

Strong proposals will offer systematic ways of exploring, describing, and excluding these phenomena where they can lead to vulnerabilities and unintended execution.

Strong proposals should recognize that format-related domain expertise is a sparse, expensive resource, and that exploring security phenomena of a complex format may require multiple experts with non-overlapping areas of expertise. TA1 proposers should discuss how they will gain sufficient access to enough of these individuals to ensure robust, accurate results. Proposals should design processes and interfaces to use the domain experts' time in the most efficient manner, by creating capabilities to automatically digest large corpora of format samples and to promptly validate or disprove hypotheses about the use (or abuse) of particular format features in the wild (as well as take TA4-developed requirements into account).

Note on Format Nesting

SafeDocs considers all data parsed within a process to be within the scope of the above definitions. For example, when an electronic data format allows inclusions of another format, to be parsed with a plugin or a library, the included format must receive the same treatment of de facto allowed syntactic analysis and simplification to allow parser verification, or be excluded from the simplified format if such exclusion does not affect the format's essential functionality.

C.2 TA2: Constructing secure parsers

Existing approaches to validation of electronic data inputs appear to be lacking a constructive theory of security. Theoretically compelling approaches, such as defining an electronic data format via a formal grammar, fail to address popular extant formats (due to their complexity and ambiguity), whereas approaches used in practice lack theoretical cogency (and, often, actual efficacy). As a result, security risks of interacting with untrusted complex inputs lack a theoretical basis on which they could be evaluated, while empirically these risks appear to approach those of running untrusted code.

SafeDocs requires a breakthrough constructive theory that connects input validation and security. The scope of TA2 proceeds from the following assumptions:

1. Secure handling of untrusted inputs means predictable execution driven by consumption of these inputs.
2. Input validation means automatic, static reasoning about the execution an input will produce.
3. For many models of computation driven by inputs–e.g., when the inputs are general-purpose programs or equivalents thereof, to be executed by the receiving entity–static reasoning about non-trivial properties of execution is undecidable, thus making the security of these models of input consumption in the sense of (1) and (2) undecidable.

   Such models are outside of the SafeDocs scope if their properties that lead to undecidability are intentional. For example, intentional interpretation (or compilation and execution) of inputs that are general-purpose programs or deliberate equivalents thereof is outside of SafeDocs's scope.
4. Deserialization, parsing, and validation of structured electronic data should not be one of the models in (3).

When a computation model associated with consuming an electronic data format exhibits undecidable characteristics *unintentionally*, SafeDocs views this property as an obstacle to constructing verified parsers, and seeks to remove it via safe sub-setting of the format, as discussed above. Note that well-known vulnerabilities resulted from the common anti-pattern of passing string inputs to full-featured execution environments such as command shells or general-purpose programming language interpreters, typically under the assumption that the passed strings were filtered or "sanitized" to allow only the intended command(s) and none others. SafeDocs regards general-purpose code injection and execution resulting from this anti-pattern as unintentional and calls for identifying and eliminating all of its instances in the electronic data formats under scrutiny. This phenomenon is one of many that underscore the importance of empirical format exploration involving domain experts. Strong proposals should address this phenomenon.

Consistent with the TA1 note on format nesting, SafeDocs regards all electronic data formats that can be contained in a format and are parsed within the same process to be within scope as defined by assumptions 1-4 above.

SafeDocs thus requires the co-design of electronic data formats and the code that parses and validates these data formats to allow static reasoning about the effects of consuming inputs. For extant formats, it calls for principled safe sub-setting of the format's syntax to allow such reasoning.

Outcomes of TA2

This technical area of SafeDocs will produce:

a) constructive theories of security for parsers;
b) secure parser construction kits usable by industry programmers who understand the format but lack the theoretical background in verified programming;
c) verified parsers for selected extant electronic data formats, given their simplified verification-enabling subset definitions developed in TA1, and produced with the use of the secure parser construction kits (b); and
d) for electronic data formats subject to de facto syntax extensions, high-assurance translators from the de facto syntax to the simplified syntax, based on the transformations developed in TA1.

More specifically, SafeDocs poses the following theory, design, and instantiation challenges.

Theory Challenge: A Theory of Input Validity

Strong TA2 proposals will present a formalism to capture the idea of input validity understood as a decidable property of the input (and of the input-checking code) that can be checked efficiently, by code that can be proved correct, and, having been checked, provides security guarantees to the rest of the program's code modules. These security guarantees should amount to preclusion of unintended computation due to consumption of inputs both while their validity is being checked and after it has been checked (and the input has not been rejected as invalid).

For example, should the modules of a program downstream of the input checker be verified in turn, the input checker will provide preconditions for their verification, sufficient to show that no unintended computation will occur due to consumption of successfully validated inputs.

The theory of input validity will offer insights on the complexity of input validation and of verifying implementations of input validation. It will warn of flawed designs where the validity of inputs offers no security value in the sense of precluding unintended computation, or implies that effective validation of inputs means solving undecidable problems.

TA2 proposals that explore several competing or complementary formal approaches should describe each approach as a separate statement-of-work task and provide sufficient costing details for such tasks to be separable.

Bringing Secure Parsing Development Kits to Industry Developers

SafeDocs will develop approaches and tools for creating high-assurance parsers. ***These tools will be accessible to industry developers, and will make secure, succinct, and efficient parsing code faster to write, to test, and to run.*** These tools will build on the recent advances in parser programming, leveraging programming language constructs familiar to developers, and making use of intelligible, constructive, and prompt feedback from the development tool chain components (such as an Integrated Development Environment (IDE)) to guide the developers.

Parser code should make it immediately clear which syntactic element of input is being consumed by any particular line of the code, and which properties of input have been checked, are being checked, and are yet to be checked at every line. Answering these questions, e.g., during a code review or a security audit, should not require a static analysis tool – the answers should be obvious from the code itself, to a human or a machine.

A strong TA2 proposal should outline the current state of the art in regard to at least the following challenges, identify weaknesses of current approaches, and plan to address them.

Usability: Developer's learning curve for the new programming idioms should be minimized, maximizing their productivity. Using the proposed style of parser programming should make parsers faster to write and easier to read than "rolling one's own parsers."[1]

Intelligibility: If using a DSL to automatically generate parser code, the proposers are encouraged to keep the generated code readable and idiomatic, so that reading the syntactic specification of valid or expected data off of the generated code remains a simple non-heuristic task for both humans and machines.

Performance: Compiled code should not run significantly slower or require significantly more memory than legacy parser code.

Semantic Actions Safety: Although the user should be allowed to supply semantic action code to compose with the parser, this composition should not be allowed to compromise the parser security guarantees (as established by the input validity theory). The acceptable semantic action code can be limited, but the limitations must be made easy for the user to grasp.

Feedback: While expressive enough to capture most useful syntactic features, the declarative style should discourage security pitfalls in programming and design by giving feedback to the programmer in the form of readable warnings, instant hints from the IDE, or a combination thereof. Problematic code should be reported to the user as early as possible. The lack of a simple way to express a syntactic property should clearly signal to the user that this syntactic property is problematic.

Stability: The developers' workflow should not be brittle with respect to versions of verification tools involved "under the hood."

[1] Thus pointer-stepping parsing code such as `*hbtype = *p++;` is severely discouraged, and no one who implements a parser should have to write it ever again.

A strong TA2 proposal should consider means of steering industry developers towards the style of programming that is both intuitive given the understanding of the data format and provides maximum benefit for verification of the resulting code. Industry developers should receive intelligible, actionable feedback on the preferred idioms to accomplish the task.

Theory Outcomes of TA2 for Analysis of Electronic Data Formats

A common problem in practical security is to distinguish legacy technologies that present insurmountable security risks and must be discontinued from those for which applying mitigations may be sufficient. Recent decisions by major vendors to disable support for legacy web technologies such as Java applets or Flash suggest that the security risk-benefit analysis may no longer be always in favor of backward compatibility. However, to date, such risk-benefit analysis lacks a theoretic foundation. TA2 will help establish such foundations for data formats.

In particular, a successful input validity theory will connect validity with predictability of execution driven by inputs. The theory will distinguish between the concepts and designs of input where such predictability of computation is driven by the inputs. For example:

- Predictability cannot be achieved because the input is meant to describe general purpose computation (i.e., the input is deliberately used as a programming language for a Turing-complete computing environment, and thus automatic validation of the execution's non-trivial properties including termination is undecidable).
- Predictability cannot be achieved with the input language as described because it is accidentally Turing-complete on the accepting environment, but can, in fact, be achieved for a subset of the language and with changes to the environment.
- Predictability can be achieved, but further sub-setting of the language or the environment as above will make the checker or the verification of the checker much more efficient.
- Predictability can be achieved without changes and is, in fact, optimal among competing input formats.

Strong TA2 proposals should address metrics for complexity of new formats (a “complexity tax”) and extant formats (a “security debt”) that facilitate risk-benefit analysis of their security.

C.3 TA3: Testing and Evaluation

TA3 will evaluate assurance provided by parsers and translators developed in TA2 against best-of-breed exploitation methods, and will develop general methodologies for systematic testing of parser implementations. TA3 will test essential content and functional equivalence of documents transformed by high-assurance translators to a syntactically simpler safe subset of the format (as produced by the methodology developed in TA1).

TA3 proposals will outline the state of the art in parser testing, identify weaknesses of current approaches, and plan to address them, also planning to utilize the insights developed in TA1 and TA2.

TA3 will work with TA4 to select the appropriate electronic data formats for evaluating the progress of TA1 and TA2 performers, to ensure that the theories and technologies developed are relevant to the safe information exchange requirements established by TA4. The formats selected should represent both electronic document and data streaming use cases.

Strong TA3 proposals should outline methods for collecting and synthesizing extant data content sufficient to exercise both the static and streaming use cases for TA1 and TA2. This includes creating large (10^6 – 10^9 samples) reference corpora for selected static and streaming electronic data formats and frameworks for testing against these corpora. The reference corpora will scale with time to match the progression of program evaluation metrics (see Table 2). Reference corpora will be provided to TA1 and TA2 performer for white-box testing of their systems for correctness and coverage. An initial reference corpus of no less than 10^5 instances will be provided early within Phase 1 of the program.

In addition, TA3 will produce static and streaming testing corpora, not shared with the TA1 and TA2 performers, to test their systems for robustness with synthetic data instances during evaluation exercises.

As a key part of its mission, TA3 will orchestrate empirical exploration of the extant data formats, by engaging format exploitation and reverse engineering experts, and working with TA1 performers to ensure the discovered phenomena are accounted for in their analysis of the format. Strong TA3 proposals should demonstrate knowledge of the empirical data exploration domain and activities, and the ability to quickly and efficiently engage format experts, including non-traditional performers.

TA3, in collaboration with TA4, will produce a workbench of representative platforms on which the performance of tools developed in TA1 and TA2 will be evaluated, and will make this workbench available to the TA1 and TA2 performers within the first six months of Phase 1. TA3 will design and implement scenarios and software for the evaluation exercises.

A successful TA3 proposal should include, at a minimum, the following:

- develop automated ways to compare security assurance of parsers and translators created in TA2 against leading commercial products and open source solutions in format security;
- develop corpora, use cases, hackathon scenarios, and testing frameworks for selected extant electronic data formats, to test TA1 and TA2 solutions;
- develop automatic means of testing content equivalence between extant electronic data instances and their syntactically simplified versions as produced by TA2 translators; and develop automated ways of testing for *parser differentials*, i.e., differences in syntactic interpretations of the same message between different implementations of the same format, which generalize to classes of messages differently interpreted and manipulable by attackers.

TA3 will lead the demonstrations, the hackathons, and the exercises as described in the Program Evaluation section. The TA3 performer will submit plans for these events to the Government team at least two months prior to each event. TA3 proposers should discuss how they will facilitate these events, including the acquisition and provisioning of appropriate event facilities and resources.

Additionally, TA3 will design and implement yearly contests open to the public at information security conferences such as DEFCON, in which the developed technologies from TA1 and TA2 as well as a variety of current commercial products and open source solutions will be exposed to contestants, to gauge the progress of the SafeDocs technologies.

C.4 TA4: Instantiation

TA4 will collect business requirements for enterprise/ Internet of Things (IoT) electronic data formats, the industry development process for the code handling these formats, and for the acceptance testing of such code. TA4 will collaborate with TA1 and TA2 performers to ensure that the theories and the resulting systems developed can meet the requirements, and that the requirements are relevant to the safe information exchange needs of the public, the enterprise, and the U.S. Government agencies including the Department of Defense (DoD).

TA4 will identify industry partners interested in the eventual adoption of SafeDocs technologies, and facilitate their interaction with TA1 and TA2 performers to inform their theories. TA4 will ensure that TA1 and TA2 performers' risk-benefit analysis of electronic data format features is informed by the industry requirements, e.g., inform TA1 and TA2 of the value of risky features to industry.

TA4 will identify electronic data formats in the areas of documents, messages, and data streams that are of high security concern, and will analyze these formats using tools developed in TA1. Using tools developed in TA2, TA4 will implement prototypes of secure enclave gateways that translate these formats to their respective safe subsets, in a variety of use cases. TA4 will work with industry partners to ensure that the use cases are realistic, and the safe subsets and the gateways match the identified requirements.

TA4 performers will be expected to perform the custom programming tasks needed to adapt the tools developed in TA1 and TA2 to particular use cases of the secure enclave prototypes. TA4's feedback on usability of the tools will be the means of evaluating progress of TA1 and TA2 performers on these TA's respective usability requirements.

Using theory insights and formalisms developed in TA1 and TA2 and the experience of the use cases, TA4 will develop methodologies for code and data review suitable for use in enterprise/IoT software acceptance testing. Feedback from this effort will inform the theories developed in TA1 and TA2. TA4 performers will collaborate with TA1 and TA2 performers to produce metrics for evaluating the risks associated with legacy electronic data formats data and legacy code for handling these data formats.

In particular, TA4 will develop practical metrics for a "data complexity tax" applicable to new protocols and systems, and for the "data technical debt" applicable to legacy systems, to reflect the risks of electronic data format complexity on security of systems, and prioritize mitigations for risky legacy systems.

A strong proposal should include, at a minimum, the following:

- A plan for working with industry vendors to collect their security requirements for electronic data formats and parsers deployed in development and operational environments, and for the development toolchains used to develop data specifications and input-handling code.

- A plan to identify, design, and implement use cases of secure enclaves for the selected formats that are of interest to industry partners and match the identified requirements.
- A plan to experimentally evaluate the impact of SafeDocs tools for safe sub-setting electronic data formats and their parsers within enterprise/IoT environments.
- A plan to facilitate adoption of SafeDocs methodologies within these environments.

In the option Phase 3, TA4 will work with industry to standardize the simplified safe formats and will transition the components to identified government partners.

D. Program Structure

The program is anticipated to run 48 months and has been organized into three (3) phases. Phase 1 (base) will be 18 months and will explore selected electronic data formats. Phase 2 (base) will be 18 months and will scale prototype implementations that instantiate the theories. The program will conclude with a 12-month Phase 3 (transition phase option), which will be contingent on the success of the previous phases.

In Phase 1, performers will target the core structure and functionality of selected document and streaming formats, without restrictions on the platform's resources. In Phase 2, performers will target commonly associated data formats and extensions of the selected document, and address challenges of scale and performance, such as processing the selected streaming format on a resource-constrained embedded platform. In option Phase 3, performers will transition their methodologies and tools to industry and government partners.

In Phase 1, there will be two integration/demonstration events and a final evaluation exercise at the end of the phase. Exercises will feature test corpora not provided to performers a priori. Phase 2 and the option Phase 3 will have two demonstration events each to identify and correct any weaknesses, and provide ample time to address any shortcomings before mid-phase and final evaluation exercises. (See Figure 1.)

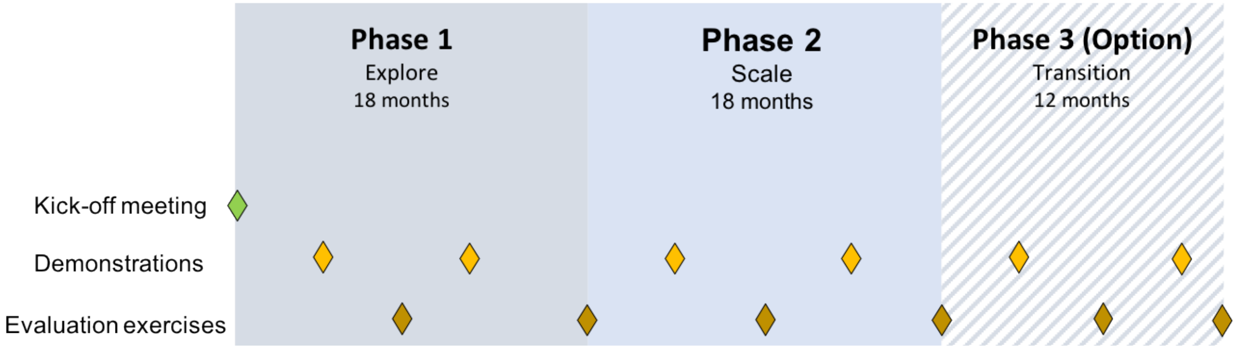


Figure 1 - Tentative evaluation schedule

Each abstract and proposal submitted against this solicitation shall address only one TA. Organizations may submit multiple abstract/proposals to any one TA, and they may propose to multiple TAs. A proposer submitting a proposal to TA1 and another to TA2 may be selected to perform on both TAs. However, TA3 and TA4 performers cannot perform on any other TA.

There are multiple points of expected and potential collaboration among TAs, and the Government expects that all performers producing software will interact closely with the TA3 (evaluation) and TA4 (instantiation) performers. Additionally, TA1 and TA2 performers are expected to collaborate closely, as described below. Proposers should read the descriptions of all TAs and the Program Evaluation and Demonstration section to ensure a full understanding of the program context, structure, and anticipated relationships required among performers. To facilitate the open exchange of information, all program performers will have an Associate Contractor Agreement (ACA) language included in their award.

TA4 will lead the development of the ACA for the program. See Section VIII.E for more information regarding the ACA.

There will be no forced downselects in phases 1 and 2, but continued funding will depend on demonstrated progress in achieving program goals.

Efforts in the four technical areas of this program run concurrently, with ramp-up and ramp-down for specific tasks, as described below. Relationships between the technical areas change from phase to phase, as described below.

Phase 1: Explore

In phase 1, TA1 performers will focus on creating the tool chain and methodology for comprehending an extant electronic data format (the "challenge format"). In the meantime, TA2 performers develop the theory and build up tools for their verified parser construction kits using a series of simpler format descriptions, already formulated in machine-readable form, which approximate the initial output of TA1 efforts in this phase.

The TA1 toolchain will include tools for:

a) representing the format specification in a machine-readable form;
b) recovering the de facto language(s) allowed by implementations, from source code or binary (this includes effective automation for exploring differences between (a) and the implementation); and
c) enumerating format features and their uses in a large corpus of documents and effective automation for checking whether any properties encoded in (a) and (b) hold for the documents in the corpus, and effectively summarizing where and how they are violated if not.

It is anticipated that these tools will be developed in parallel with comprehending the challenge format, co-evolving with the comprehension effort, and, by the end of Phase 1, will produce comprehensible, machine-readable description of the format syntax used to express the core format functionality, and this syntax will be suitable for verified programming use in TA2.

Throughout Phase 1, and especially in its second sub-phase, TA1 performers are expected to collaborate with TA2 performers to assure suitability of their output to TA2.

The syntax and semantics of the TA1-produced human-and-machine-readable specification are expected to largely settle by the end of Phase 1, although its further evolution is expected through Phase 2; it is expected to reach beta state in the middle of Phase 2. At the start of Phase 3, it is expected to reach the release candidate state (and meet with approval by TA4 performers).

Meanwhile, TA2 performers are expected to start developing infrastructure for building verified parser construction kits, to take advantage of the data format specifications being developed in TA1.

The goal for TA2 performers in Phase 1 is to build up the capability to construct provably correct parsers for simple data formats described by an unambiguous and human-intelligible specification that is also machine-readable. TA2 performers will build on this capability in Phase 2, to construct and verify more complex parsers for more complex formats, as machine-readable specifications for these are created in TA1.

Usability of the parser construction kits will be a focal point for TA2. TA4 and TA3 performers will provide continuous feedback to TA2 performers. Performance optimization (so long as the overhead of the kit-based parsers is within the allowed percentage of the metrics for Phase 1) will become a focal point in Phase 2.

TA3 performers will evaluate parsers produced in TA2 and specifications produced in TA1 for the metrics of Phase 1.

TA4 performers will collect requirements defining enterprise/IoT use of electronic document, message, and streaming formats, ensuring that the instantiation of data validity and verified code theories developed in TA1 and TA2 address these requirements.

Phase 2: Scale

In Phase 2, the TA2 focus shifts to developing verified parsers using the de facto format specification being recovered in TA1. TA1 continues to refine its toolchain, and, in this phase, applies it to a variety of formats to complete the recovery of the ground truth in the challenge suite of extant, populated electronic data format, to scale its performance to larger corpora of extant documents, and to improve its accuracy, as per Phase 2 metrics.

In this phase, the fitness of specifications produced in TA1 for the verified parser programming approaches being developed in TA2 is put to the test. Although TA2 performers are expected to provide feedback on the format of the TA1 outcomes throughout Phase 1, it in Phase 2 that TA2 performers receive a synthesized “ground truth” description of a complex format and must accommodate it with their verified parser construction kits (or push back with rigorous arguments of why such accommodation is not possible, so that TA1 tools could be modified to allow it).

Usability of TA2’s verified parser construction kits remains a concern in Phase 2, but performance of the produced code becomes a focus. TA2 performers are expected to release their secure parser construction tool kits to the TA4 performer “early and often,” to seek TA4’s feedback.

TA3 will continue developing and testing the means of evaluation of security and performance of the parsers.

TA4 will ramp up work to instantiate the prototype of a secure enclave entry gateway, combining machine-readable format descriptions produced in TA1 with tools being developed in TA2.

Phases 1 and 2 are expected to explore competing approaches to their technical areas, since the current state of theory does not allow pre-selecting them. In fact, one of the desired outcomes of TA1 and TA2 should be the creation of such theories. By the end of Phase 2, leading approaches should emerge.

Phase 3: Transition (Option)

In Phase 3, the focus moves to TA4's instantiation effort and TA3 testing. TA1 and TA2 will serve to support the instantiation. TA4 will ramp up, and TA1 will ramp down. TA2 will focus on optimization and scalability.

In particular, the TA4 performer will field the secure parser construction technologies developed in TA2 with industry developers who are not verification experts and are not familiar with verification theory. These developers will use the tools developed in TA2 to implement a performant gateway for a protected enclave and test it on a large corpus of internal documents and messages in the selected format, applying the tools developed in TA1 to diagnose any documents that fail to pass the gateway. TA1 and TA2 teams will support the effort and modify the tools as needed.

Collaboration

Close collaboration is expected on this effort. Proposers of TA1 and TA2 will have to work closely to coordinate common data representations and languages for the de facto syntax of extant electronic data formats, the simplified safe-subset syntax of these formats, and for the translation from the former to the latter. TA1 and TA2 performers will have to work closely with the TA4 performer to satisfy the respective usability requirements for their tools and methodologies. A more detailed table and a diagram of expected collaborations are provided below to call attention to a subset of the expected touch-points between performers. An understanding of the metrics used to evaluate every TA will help inform the responsibilities and dependencies between performers.

A subset of collaboration deliverables includes the following:

From	Provides	To
TA1	specification of extant format's de facto syntax	TA2
TA1	safe subset of format syntax	TA2
TA1	translation rules from de facto to safe syntax	TA2
TA2	verified programming requirements on safe syntax	TA1
TA2	secure parser construction kits	TA4
TA2	verification tools for kit-derived parsers	TA4
TA4	usability feedback	TA2
TA4	performance requirements and feedback	TA2
TA3	reference corpora, pre-testing	TA1, TA2
TA3	test corpora, not a priori available	TA1, TA2
TA3	select format specification, Phase 1	TA2
TA3	resource constrained testing platform, Phase 2	TA2
TA4	testing platform requirements	TA3

Table 1 - Expected interactions and touch-points

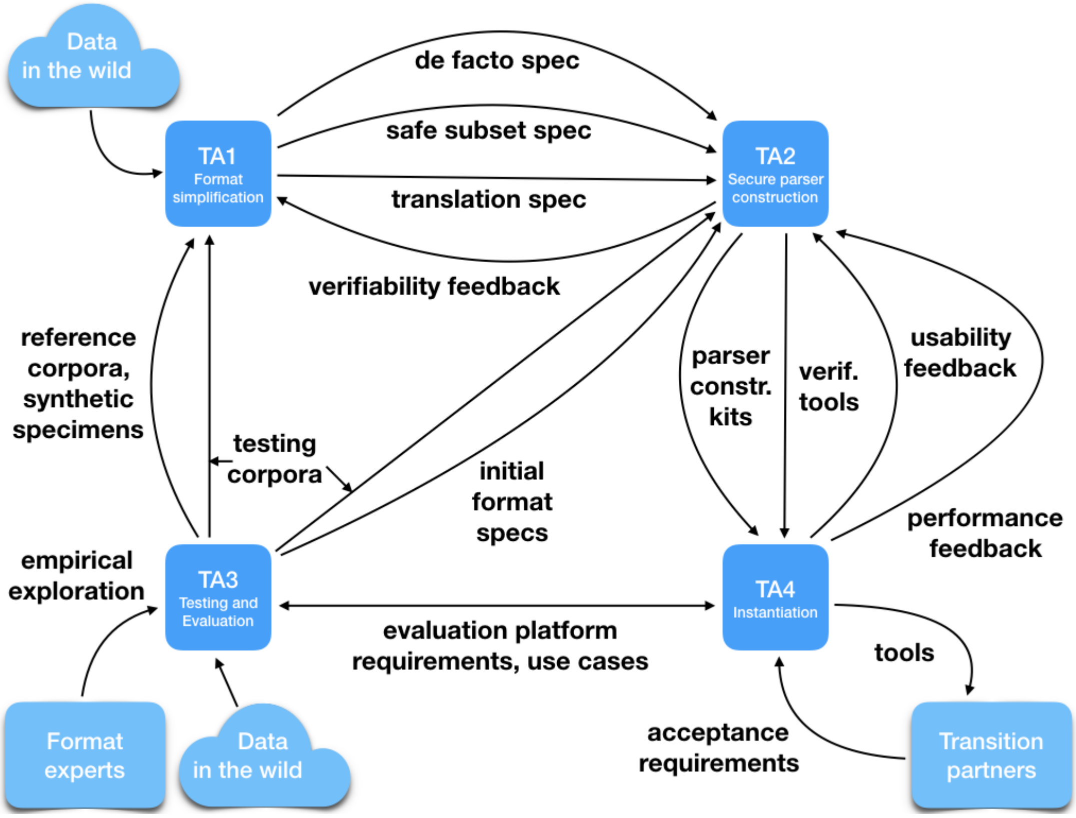


Figure 2 - Depiction of expected interactions and touch-points

E. Program Evaluation and Demonstration

The TA3 performer (evaluator) and the TA4 performer (instantiator) will assist the Government team in the development of evaluations to provide feedback to TA1 and TA2 performers. These evaluations will include demonstrations of the SafeDocs methodologies and tools for selected extant electronic data formats and corpora for these formats to characterize the capabilities that TA1 and TA2 performers produce.

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 SafeDocs program objectives. *Table 2* (on the next page) outlines the envisioned metric progression.

	Phase 1	Phase 2	Phase 3 (option)
	Explore	Scale	Transition
Corpus size	10^5 documents	10^6 documents	10^8, scaling to 10^{10}
TA1: Format simplification			
Data Formats	PDF core structure and functionality; DDS streaming data format (TBD), no CPU restriction.	PDF with commonly associated* data formats and extensions; Streaming data format, on an embedded platform with limited resources.	PDF with full set of enterprise features; Streaming format, embedded platform, real time.
Automation	Manual	Automated, with human in the loop	Automatic, with minimal human annotation
False positive allowed (benign docs rejected)	< 10%	< 1%	< 0.01%
TA2: Safe parser construction			
Software produced and modified	Prototype, single compiler/build chain	Compiler IDE, single language and libraries	Multiple languages and IDEs
Code succinctness when using new tools	50% of comparable legacy code size	20%	10%
Defects allowed in commodity code	1-5 per KLoC (industry's average: > 10-20/KLoC)	< 0.5 per KLoC (industry's best: 0.5/KLoC)	< 0.1 per KLoC (cf. current clean room code: 0.1)
Performance overhead	< 30%	< 10%	< 5%

* The list of commonly associated data formats will come from TA1 Phase 1 analysis.

Table 2 – SafeDocs program metrics

Strong TA2 proposals will discuss additional metrics that measure the security improvement over available approaches and tools.

All TA1 and TA2 proposals must describe a set of metrics specific to the proposed approach. In the first two months of the program, each performer will collaborate with TA3 and TA4 to produce a document defining the metrics for measuring their system's performance in addition to those in *Table 2*.

The evaluator (TA3) will develop and conduct largely automated testing on a two-month basis to verify that each system builds and executes its tests properly. Each performer developing software will receive testing reports to assist their development efforts. Over the course of Phase 1, TA3 will build out their own test cases for each system, to augment performer-provided tests.

F. Demonstrations, Exercises, and Hackathons

Program meetings, beyond the initial program kick-off meeting, consist of two types: *demonstrations* and *exercises*.

Demonstrations are smaller, SafeDocs-internal events that focus on facilitating performer collaborations. Demonstration events start at six months and are used to provide feedback to the TA performers to guide research and development efforts. Each demonstration will provide the

Government team a chance to see the methodologies and tools under development being applied to corpora of extant data formats. Reference corpora will be provided by the TA3 performer to all performers and accessible for testing and development purposes prior to the demonstration.

Demonstrations will start with a 2-day *hackathon* followed by a 1.5-day *Principal Investigator* (*PI) meeting* held at the same location. The **hackathons** will enable the Government to gauge the progress of the methodologies developed in TA1 and TA2 towards making secure, efficient parsing code faster to write, to test, and to run, by having the hackathon participants collectively engage in these activities. TA3 will provide challenge problems to be solved during the hackathons, such as accommodating an extension of the selected format. The performers will apply their tools to solve these problems within the allotted time. Hackathons will focus on open technical exchange that includes discussion of difficulties encountered and possible solutions. The goals of the hackathons will be to: (a) review and share innovations/accomplishments of the program; (b) review and discuss plans and options for the exercises; (c) review and discuss results from meetings and events conducted prior to the tests and evaluations; (d) demonstrate prototypes; and (e) plan for the following evaluation. Hackathons will be followed by PI meetings in the same location. During these meetings, PIs will discuss the outcomes of the hackathons and plan further collaboration.

Initial demonstrations will not be platform-restricted. However, in Phase 2, the focus will shift to reference platforms that represent requirements identified by TA4.

Exercises are larger, one-week events with more Government engagement that focus on evaluating performer progress. Exercises consist of challenge tasks and scenarios that increase in scale and realism over the course of the program. Corpora to be used in exercises (from TA3) will not be provided to the performers a priori. Test corpora will include synthetic malformations in the electronic data format instances, which should be handled safely by the developed software prototypes. TA3 will lead the development of the testing scenarios for the exercises, and work with TA4 to ensure their increasing relevance to industry and Government partners. TA3 will be responsible for provisioning of appropriate event facilities and resources for the demonstrations (including hackathons) and exercises.

There will be twelve total demonstrations and exercises over the life of the program (counting the option Phase 3). DARPA will arrange to have Government subject matter experts (SMEs) participate in each of these exercises to help performers understand the domains of use for the respective electronic data formats in sufficient detail. These SMEs will execute non-disclosure agreements (NDAs) with SafeDocs performers.

For costing purposes, assume that demonstrations will take place in the Washington, D.C. metro area. The first two demonstrations will be attended by the majority of each team’s personnel, to gain familiarity with the domain.

Proposers should assume that the first exercise will take place in the Washington D.C. metro area, and will be attended by the majority of each team’s personnel. Each of the remaining exercises will require at least three technical team members to be onsite at the event location for one week. For costing purposes, assume that the locations of exercises will alternate between San Diego, CA, Knoxville, TN, and the Washington, D.C. metro area.

The Government will specify the dates and locations for these events. Refer to the tentative schedule in Figure 1.

G. Deliverables to DARPA

All performers will be required to provide, at a minimum, the following deliverables:

- Any technical papers derived from work funded by SafeDocs.
- Commented source code, any other necessary data and documentation (including at minimum user manuals and a detailed software design document) for all software developed under this program.
- For all performers developing software (TA1, TA2), code/data drops will be provided to the Evaluator (TA3) every two months, to include all source code, build scripts, test harnesses, development environments, unit tests and system tests.
- For all performers developing software (TA1, TA2), in the first two months of each phase (60 calendar days), a document defining metrics for testing and evaluation and discussing a concept of operations for conducting evaluations of any software that requires user interaction, to be produced in collaboration with the Evaluator (TA3).
- Annotated slide presentations must be delivered within one month after kickoff meeting and after each program event (hackathons, demonstrations and evaluations).
- Quarterly technical status reports detailing progress made, tasks accomplished, major risks, planned activities, trip summaries, changes to key personnel, and any potential issues or problem areas that require the attention of the Government Team must be provided within 10 calendar days of the end of each quarter.
- Monthly financial status reports must be provided within 10 calendar days of the end of each calendar month.
- A final phase report for each program phase that concisely summarizes the effort conducted, technical achievements, and remaining technical challenges will be due 30 calendar days after the end of each phase.
- A final report at the end of the overall period of performance that summarizes the project.

H. 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 VI.B.1 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, hardware designs and documentation, and technical data generated by the program be provided as deliverables to the Government, 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. Awards

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

The Government reserves the right to:

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

Proposals selected for award negotiation may result in a procurement contract, cooperative agreement, or Other Transaction (OT) depending upon the nature of the work proposed, the required degree of interaction between parties, and other factors. Grants will NOT be awarded under this program.

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

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

In all cases, the Government contracting officer shall have sole discretion to select award instrument type, regardless of instrument type proposed, and to negotiate all instrument terms and conditions with selectees. DARPA will apply publication or other restrictions, as necessary, if it determines that the research resulting from the proposed effort will present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Any award resulting from such a determination will include a requirement for DARPA permission before publishing any information or results on the program. For more information on publication restrictions, see the section below on Fundamental Research.

B. Fundamental Research

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

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

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

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

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

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

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

DFARS 252.204-7000, "Disclosure of Information"

DFARS 252.204-7008, “Compliance with Safeguarding Covered Defense Information Controls”
DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”

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

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

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

III. Eligibility Information

A. Eligible Applicants

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

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

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

a. FFRDCs

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

b. Government Entities

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

c. Authority and Eligibility

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

2. Foreign Participation

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

B. Organizational Conflicts of Interest

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

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

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

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

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

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

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

C. Cost Sharing/Matching

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

D. Other Eligibility Requirements

Each abstract and proposal submitted against this solicitation shall address only one TA. Organizations may submit multiple abstract/proposals to any one TA, or they may propose to multiple TAs. A proposer submitting a proposal to TA1 and another to TA2 may be selected to perform on both TAs. However, TA3 and TA4 performers cannot perform on any other TA.

IV. Application and Submission Information

A. Address to Request Application Package

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

B. Content and Form of Application Submission

1. Abstracts

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

- What is the proposed work attempting to accomplish or do?
- How is it done today, and what are the limitations?
- Who will care and what will the impact be if the work is successful?
- How much will it cost, and how long will it take?

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

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

Reminder – Each abstract submitted in response to this BAA shall address only one TA. Organizations may submit multiple abstracts to any one TA, or they may submit abstracts to multiple TAs.

All pages shall be formatted for printing on 8-1/2 by 11 inch paper with 1-inch margins and font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts. Document files must be in **.pdf** or **.xlsx** formats without scripts, macros, SMB or Dynamic Data Exchange (DDE) references, XML externals entities, or similar. Submissions must be written in English. All pages should be numbered.

Abstracts must include the following components:

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

- **Goals and Impact:** Describe what is being proposed and what difference it will make (qualitatively and quantitatively) if successful. Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the relationship of this work to any other projects from the past and present.

- **Technical Plan:** Outline and address all technical challenges inherent in the approach and possible solutions for overcoming potential problems. Provide appropriate specific milestones (quantitative, if possible) at intermediate stages of the project to demonstrate progress.

- **Capabilities/Management Plan:** Provide a brief summary of expertise of the team, including subcontractors and key personnel. Identify a principal investigator for the project and include a description of the team’s organization including roles and responsibilities. Describe the organizational experience in this area, existing intellectual property required to complete the project, and any specialized facilities to be used as part of the project. List Government-furnished property, facilities, or data assumed to be available. If desired, include a brief bibliography with links to relevant papers, reports, or resumes of key performers. Do not include more than two resumes as part of the abstract. Resumes count against the abstract page limit.

- **Statement of Work, Cost and Schedule:** Provide a cost estimate for resources over the proposed timeline of the project, broken down by year. Include labor, materials, a list of deliverables and delivery schedule. Provide cost estimates for each subcontractor (may be a rough order of magnitude).

2. Proposals

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

All pages shall be formatted for printing on 8-1/2 by 11-inch paper with 1-inch margins, single-line spacing, and a font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts. Document files must be in **.pdf** or **.xlsx** formats without scripts, macros, SMB or DDE references, XML externals entities, or similar. Submissions must be written in English. All pages of Volume 1 should be numbered.

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

Reminder – Each proposal submitted in response to this BAA shall address only one TA. Organizations may submit multiple proposals to any one TA, or they may propose to multiple TAs.

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

a. Volume 1: Technical and Management Proposal

The maximum page count for Volume 1 is 40 pages, including all figures, tables and charts but not including the cover sheet, table of contents or appendices. A submission letter is optional and is not included in the page count. Appendix A does not count against the page limit and is mandatory. Appendix B does not count against the page limit and is optional. Additional information not explicitly called for here must not be submitted with the proposal, but may be included in the bibliography in Appendix B. Such materials will be considered for the reviewers' convenience only and not evaluated as part of the proposal.

Volume 1 must include the following components:

i. Cover Sheet: Include the following information.

- Label: "Proposal: Volume 1"
- BAA number (HR001118S0054)
- Technical Area
- Proposal title
- Lead organization (prime contractor) name
- Type of organization, selected from the following categories: Large Business, Small Disadvantaged Business, Other Small Business, HBCU, MI, Other Educational, or Other Nonprofit
- Technical point of contact (POC) including name, mailing address, telephone, and email
- Administrative POC including name, mailing address, telephone number, and email address
- Award instrument requested: procurement contract (specify type), cooperative agreement or OT[2]
- Total amount of the proposed effort
- Place(s) and period(s) of performance
- Other team member (subcontractors and consultants) information (for each, include Technical POC name, organization, type of organization, mailing address, telephone number, and email address)
- Proposal validity period (minimum 120 days)
- Data Universal Numbering System (DUNS) number[3]
- Taxpayer Identification Number (TIN)[4]

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

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

[4] See http://www.irs.gov/businesses/small/international/article/0,,id=96696,00.html for information on requesting a TIN. Note, requests may take from 1 business day to 1 month depending on the method (online, fax, mail).

- Commercial and Government Entity (CAGE) code[5]
- Proposer's reference number (if any)

ii. Table of Contents

iii. Innovative Claims and Deliverables: Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the uniqueness and benefits of this project in the context of the state of the art, alternative approaches, and other projects from the past and present. Describe how the proposed project is revolutionary and how it significantly rises above the current state of the art.

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

iv. Technical Plan: Outline and address technical challenges inherent in the approach and possible solutions for overcoming potential problems. Demonstrate a deep understanding of the technical challenges and present a credible (even if risky) plan to achieve the project's goal. Discuss mitigation of technical risk. Provide appropriate measurable milestones (quantitative if possible) at intermediate stages of the project to demonstrate progress, and a plan for achieving the milestones.

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

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

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

Include a table of key individual time commitments as follows:

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

vii. Capabilities: Describe organizational experience in relevant subject area(s), existing intellectual property, or specialized facilities. Discuss any work in closely related research areas and previous accomplishments.

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

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

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

x. Appendix A: This section is mandatory and must include all of the following components. If a particular subsection is not applicable, state “NONE”.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Please also complete the following statements.

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

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

(9). Cost Accounting Standards (CAS) Notices and Certification: For any proposer who submits a proposal which, if accepted, will result in a CAS-compliant contract, must include a Disclosure Statement as required by 48 CFR 9903.202. The disclosure forms may be found at http://www.whitehouse.gov/omb/procurement_casb.

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

xiii. Appendix B. If desired, include a brief bibliography to relevant papers, reports, or resumes. Do not include technical papers. This section is optional, and the materials will not be evaluated as part of the proposal review.

b. Volume 2 - Cost Proposal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(6) ODCs: Provide an itemized breakout and explanation of all anticipated other direct costs.

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

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

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

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

v. Proposals Requesting an Other Transaction Agreement: Proposers must indicate whether they qualify as a nontraditional Defense contractor[6], have teamed with a nontraditional Defense contractor, or are providing a one-third cost share for this effort. Provide information to support the claims.

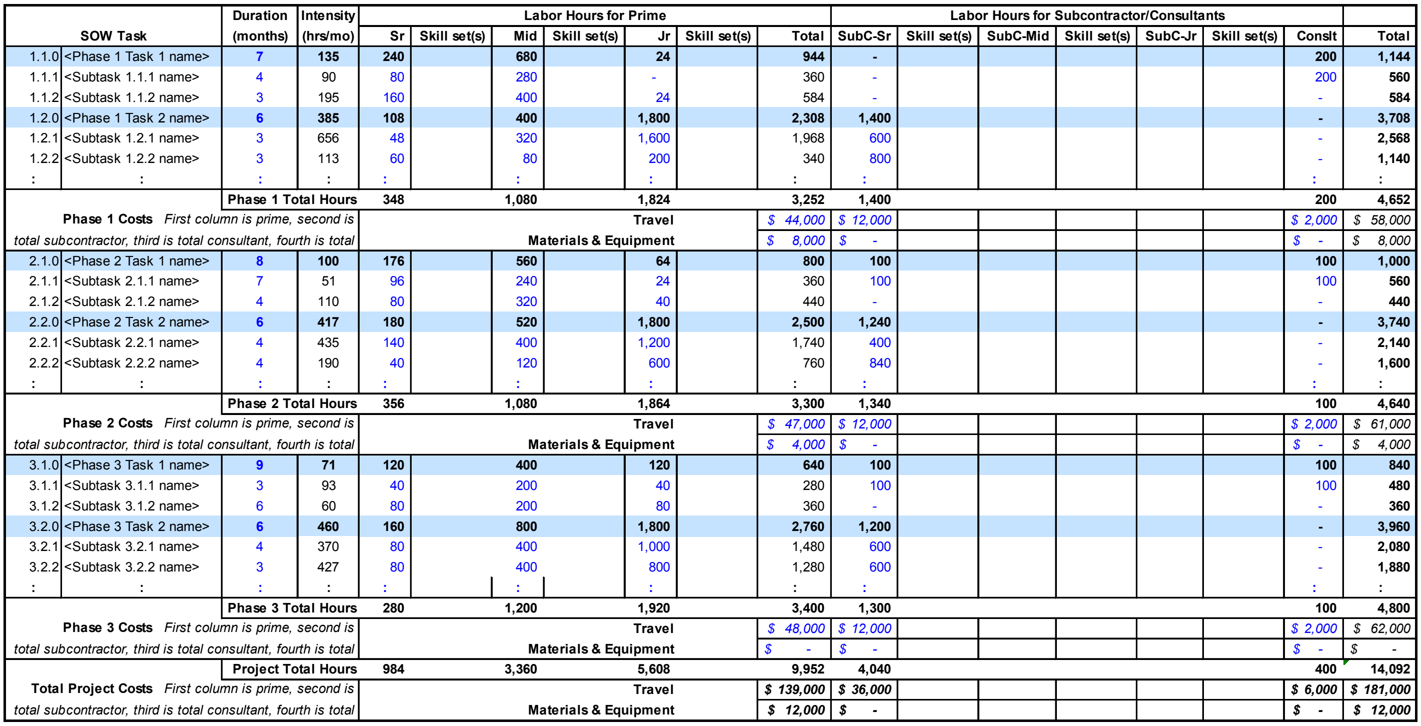
Provide a detailed list of milestones including: description, completion criteria, due date, and payment/funding schedule (to include, if cost share is proposed, contractor and Government share amounts). Milestones must relate directly to accomplishment of technical metrics as defined in the solicitation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

c. Level of Effort Summary by Task Spreadsheet

Provide a one-page table summarizing estimated level of effort per task (in hours) broken out by senior, mid-level, and junior personnel, in the format shown below in Figure 3. Also include dollar-denominated estimates of travel, materials, and equipment. For this table, consider materials to include the cost of any data sets or software licenses proposed. For

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

convenience, an Excel template is available for download along with the BAA. Submit the Level of Effort Summary Excel file (do not convert the Excel file to pdf format) in addition to Volumes 1 and 2 of your full proposal. This Excel file does not count towards the total page count.



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

Figure 3 - Example level-of-effort summary table. Numbers illustrate roll-ups and subtotals. The SubC column captures all subcontractor hours and the Conslt column captures all consultant hours. The Skill set(s) columns should indicate an area of expertise (e.g., engineer, software developer, data scientist, subject matter expert).

d. Summary Slide

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

3. Proprietary and Classified Information

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

a. Proprietary Information

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

b. Classified Information

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

C. Submission Dates and Times

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

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

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

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

1. Abstracts

Abstracts must be submitted per the instructions outlined herein and received by DARPA no later than **September 7, 2018, at 12:00 noon (ET)**. Abstracts received after this date and time will not be reviewed.

2. Proposals

The proposal package -- full proposal (Volume 1 and 2) and, as applicable, proprietary subcontractor cost proposals -- must be submitted per the instructions outlined herein and received by DARPA no later than **October 19, 2018, at 12:00 noon (ET)**. Submissions received after this date and time will not be reviewed.

D. Funding Restrictions

Not applicable.

E. Other Submission Requirements

1. Unclassified Submission Instructions

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

a. Abstracts

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

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

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

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

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

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

Since abstract submitters may encounter heavy traffic on the web server, they should not wait until the day abstracts are due to request an account and/or upload the submission. Abstracts should not be submitted via Email or Grants.gov. Any abstracts submitted by Email or Grants.gov will not be accepted or reviewed.

b. Proposals Requesting a Procurement Contract or Other Transaction

DARPA/I2O will employ an electronic upload submission system (https://baa.darpa.mil/)

for UNCLASSIFIED proposals requesting award of a procurement contract or Other Transaction under this solicitation.

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

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

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

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

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

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

c. Proposals Requesting a Cooperative Agreement

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; or (2) hard-copy mailed directly to DARPA. If proposers intend to use Grants.gov as their means of submission, then they must submit their entire proposal through Grants.gov; applications cannot be submitted in part to Grants.gov and in part as a hard-copy. Proposers using Grants.gov do not submit hard-copy proposals in addition to the Grants.gov electronic submission.

Submissions: Proposers must submit the three forms listed below.

> SF 424 Research and Related (R&R) Application for Federal Assistance, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_SF424_2_0-V2.0.pdf. *This form must be completed and submitted.*
>
> To evaluate compliance with Title IX of the Education Amendments of 1972 (20 U.S.C. A§ 1681 Et. Seq.), the Department of Defense is using the two forms below to collect certain demographic and career information to be able to assess the success rates of women who are proposed for key roles in applications in science, technology, engineering, or mathematics disciplines. Detailed instructions for each form are available on Grants.gov.
>
> Research and Related Senior/Key Person Profile (Expanded), available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_KeyPersonExpanded_2_0-V2.0.pdf. *This form must be completed and submitted.*
>
> Research and Related Personal Data, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_PersonalData_1_2-V1.2.pdf. *Each applicant must complete the name field of this form, however, provision of the demographic information is voluntary. Regardless of whether the demographic fields are completed or not, this form must be submitted with at least the applicant's name completed.*

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

Once Grants.gov has received an uploaded proposal submission, Grants.gov will send two email messages to notify proposers that: (1) their submission has been received by Grants.gov; and (2) the submission has been either validated or rejected by the system. It may take up to two business days to receive these emails. If the proposal is rejected by Grants.gov, it must be corrected and re-submitted before DARPA can retrieve it (assuming the solicitation has not expired). If the proposal is validated, then the proposer has successfully submitted their proposal, and Grants.gov will notify DARPA. Once the proposal is retrieved by DARPA, Grants.gov will send a third email to notify the proposer. The proposer will then receive an email from DARPA acknowledging receipt and providing a control number.

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

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

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

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

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

V. Application Review Information

A. Evaluation Criteria

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

- *Overall Scientific and Technical Merit*:

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

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

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

- *Potential Contribution and Relevance to the DARPA Mission:*

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

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

- *Cost Realism:*

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

B. Review and Selection Process

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

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

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

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

VI. Award Administration Information

A. Selection Notices

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

B. Administrative and National Policy Requirements

1. Intellectual Property

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

The program will emphasize creating and leveraging open source technology and architecture. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open source/open architecture regimes.

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

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

a. Intellectual Property Representations

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

b. Patents

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

c. Procurement Contracts

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

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

d. Other Types of Awards

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

2. Human Research Subjects/Animal Use

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

3. Electronic and Information Technology

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

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

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

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

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

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

number, and bank phone or fax number).

C. Reporting

1. Technical and Financial Reports

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

2. Representations and Certifications

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

.

3. Wide Area Work Flow (WAWF)

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

4. Terms and Conditions

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

5. FAR and DFARS Clauses

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

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

6. i-Edison

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

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

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

VII. Agency Contacts

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

- **Technical POC:** Dr. Sergey Bratus, Program Manager, DARPA/I2O

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

- **Mailing address**:

  DARPA/I2O
  ATTN: HR001118S0054
  675 North Randolph Street
  Arlington, VA 22203-2114

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

VIII. Other Information

A. Frequently Asked Questions (FAQs)

Administrative, technical, and contractual questions should be sent via email to SafeDocs@darpa.mil. All questions must be in English and must include the name, email address, and the telephone number of a point of contact.

DARPA will attempt to answer questions in a timely manner; however, questions submitted within 7 days of closing may not be answered. If applicable, DARPA will post FAQs to http://www.darpa.mil/work-with-us/opportunities.

B. Collaborative Efforts/Teaming

It is DARPA's desire to receive comprehensive, quality responses to this solicitation. To facilitate strong, collaborative teaming efforts and business relationships, a website (https://www.schafertmd.com/darpa/i2o/SafeDocs/pd/?p=teaming) has been established. Specific content, communications, networking, and team formation are the sole responsibility of the participants. Neither DARPA nor the DoD endorses the destination web site or the information and organizations contained therein, nor does DARPA or the DoD exercise any responsibility at the destination. This website is provided consistent with the stated purpose of this solicitation.

C. Proposers Day

The SafeDocs Proposers Day will be held on August 24, 2018, in Arlington, VA. The special notice regarding the SafeDocs Proposers Day, DARPA-SN-18-71, can be found at https://www.fbo.gov/index?s=opportunity&mode=form&id=dd089906ecc1c3417a7ef399a0510cc7&tab=core&_cview=0.

For further information regarding the SafeDocs Proposers Day, including slides from the event, please see http://www.darpa.mil/work-with-us/opportunities under HR001118S0054.

D. Submission Checklist

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

✓	Item	BAA Section	Applicability	Comment
	Abstract	IV.B.1	Optional, but recommended	Conform to stated page limit.
	Obtain DUNS number	IV.B.2.a.i	Required of all proposers	The DUNS Number is the Federal Government's contractor identification code for all procurement-related activities. See http://fedgov.dnb.com/webform/index.jsp to request a DUNS number. Note: requests may take at least one business day.
	Obtain Taxpayer Identification Number (TIN)	IV.B.2.a.i	Required of all proposers	A TIN is used by the Internal Revenue Service in the administration of tax laws. See http://www.irs.gov/businesses/small/international/article/0,,id=96696,00.html for information on requesting a TIN. Note: requests may take from 1 business day to 1 month depending on the method (online, fax, mail).

	Register in the System for Award Management (SAM)	VI.B.4	Required of all proposers	The SAM combines Federal procurement systems and the Catalog of Federal Domestic Assistance into one system. See www.sam.gov for information and registration. Note: new registrations can take an average of 7-10 business days. SAM registration requires the following information: -DUNS number -TIN -CAGE Code. A CAGE Code identifies companies doing or wishing to do business with the Federal Government. If a proposer does not already have a CAGE code, one will be assigned during SAM registration. -Electronic Funds Transfer information (e.g., proposer's bank account number, routing number, and bank phone or fax number).
	Ensure eligibility of all team members	III	Required of all proposers	Verify eligibility, as applicable, for in accordance with requirements outlined in Section 3.
	Register at Grants.gov	IV.E.1.c	Required for proposers requesting grants or cooperative agreements	Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. If proposers have not previously registered, this process can take between three business days and four weeks if all steps are not completed in a timely manner. See the Grants.gov user guides and checklists at http://www.grants.gov/web/grants/applicants/applicant-resources.html for further information.

The following items apply as part of the submission package:

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

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

E. Associate Contractor Agreement (ACA)

This same or similar language will be included in contract awards against HR001118S0054. Awards other than FAR based contracts will contain similar agreement language:

(a) It is recognized that success of the SafeDocs research effort depends in part upon the open exchange of information between the various Associate Contractors involved in the effort. This ACA 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 SafeDocs 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 SafeDocs 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 SafeDocs research effort include:

Contractor	Technical Area

(End of ACA)

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