Microsystems Technology Office
Broad Agency Announcement
System Security Integrated Through Hardware and firmware (SSITH)
HR001117S0023
April 19, 2017

Table of Contents

PART I: OVERVIEW INFORMATION

- **Federal Agency Name**: Defense Advanced Research Projects Agency (DARPA), Microsystems Technology Office (MTO)
- **Funding Opportunity Title:** System Security Integrated Through Hardware and firmware (SSITH)
- **Announcement Type:** Initial Announcement
- **Funding Opportunity Number:** HR001117S0023
- **Catalog of Federal Domestic Assistance Numbers (CFDA):** Not applicable
- **Dates:** (All times listed herein are Eastern Time)
    - Posting Date: April 19, 2017
    - Proposers Day: April 21, 2017
    - FAQ Submission Deadline: May 22, 2017 at 1:00 PM
    - Proposal Due Date: June 5, 2017 at 1:00 PM
    - Estimated period of performance start: November 2017
- **Concise description of the funding opportunity**: The overall goal of the SSITH program is to develop hardware design tools to provide inherent security against hardware vulnerabilities that are exploited through software in DoD and commercial electronic systems. SSITH aims to drive research required to develop secure hardware that constrains the hardware attack surface and protects against classes of software attacks which exploit hardware vulnerabilities.
- **Anticipated Funding Available for Award**: Approximately $50M
- **Anticipated individual awards**: Multiple awards are anticipated.
- **Anticipated funding type**: 6.2
- **Types of instruments that may be awarded**: Procurement contract or other transaction
- **Agency contact:**

    Dr. Linton Salmon, Program Manager
    BAA Coordinator: HR001117S0023@darpa.mil
    DARPA/MTO
    ATTN: HR001117S0023
    675 North Randolph Street
    Arlington, VA 22203-2114

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

The Defense Advanced Research Projects Agency (DARPA) often selects its research efforts through the Broad Agency Announcement (BAA) process. This BAA is being issued, and any resultant selection will be made, using the procedures under Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016 and 2 C.F.R. § 200.203. Any negotiations and/or awards will use procedures under FAR 15.4, Contract Pricing. 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 (FedBizOpps) website, http://www.fbo.gov/. The following information is for those wishing to respond to the BAA.

The Microsystems Technology Office at DARPA seeks innovative proposals in hardware advances that protect commercial and DoD electronic systems from software-assisted attacks on hardware vulnerabilities. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

A. Background

Electronic system security has become an increasingly critical area of concern for the DoD and the broader U.S. population. Current efforts to provide electronic security largely rely on robust software development and integration. Software security development environments, methodologies, and verification have been extensively analyzed and documented; however, current security measures remain inadequate. Present responses to hardware vulnerability attacks typically consist of developing and deploying patches to the software firewall without addressing the underlying hardware vulnerability. As a result, while a specific attack or vulnerability instance is defeated, creative programmers can develop new methods to exploit software access to the remaining hardware vulnerability and a continuous cycle of exploitation, patching, and subsequent exploitations ensues. A new approach is necessary to break this cycle of hardware vulnerability exploitation.

The System Security Integrated Through Hardware and firmware (SSITH) program addresses the use of hardware security architectures to help protect systems against ***classes*** of hardware vulnerabilities, rather than focusing on single instances of software weaknesses that exploit those vulnerabilities. There are seven known ***classes*** of hardware vulnerabilities listed in the Common Weakness Enumeration (CWE) list [1]: permissions and privileges, buffer errors, resource management, information leakage, numeric errors, crypto errors, and code injection. Changes to the integrated circuit architecture could provide hardware protection against vulnerability instances by addressing the vulnerability ***classes*** at their source, the hardware.

Reference: [1] The Common Weakness Enumeration List (CWE), cwe.mitre.org

B. Program Description

The goal of the SSITH program is to develop hardware design tools that provide security against hardware vulnerabilities that are exploited through software in DoD and commercial electronic systems. SSITH seeks to leverage current research in hardware design and software security to propel new research in the area of hardware security at the microarchitecture level. Security approaches will limit the permitted hardware to states that are assured to be secure while maintaining the performance and power required for system operation.

SSITH will develop architectures and design tools that enable system-on-chip (SoC) designers to safeguard hardware against *all seven (7) known CWE **classes** of hardware vulnerabilities* that can be exploited through software. A summary of these CWE classes is included in Attachment 3. SSITH aims to drive research required to develop secure hardware that constrains the hardware attack surface and protects against classes of software attacks which exploit hardware vulnerabilities. Development and demonstration of design tools will greatly facilitate wide use of SSITH security concepts. It is expected that architectures and design tools developed through this program will provide robust and flexible solutions applicable to both DoD and commercial electronic systems.

SSITH encourages proposals that utilize security concepts to drive development of security architectures and design tools. Listed below are examples of a few of the security concepts that may be incorporated in a security architecture.

- Cryptography
- Metadata tagging
- Formal verification
- Verified state matching
- Anomalous state detection
- Secure multi-party computing
- Semi-homomorphic computing
- Security through compartmentalization

SSITH will drive demonstration and evaluation of selected security architectures through red team evaluation and comparison to security metrics. Security architectures will be instantiated in custom hardware to demonstrate the security of the resulting systems as well as to evaluate the impact of securitization on the performance, power, area, software compatibility, and security (PPAS) of resulting systems.

SSITH security architectures are intended to be capable of being implemented in such a way that existing application software can be run on securitized hardware without software modification. It is expected that some software modification may be required to fully exploit hardware security features, but security should be maximized for unmodified software and software modification required to fully exploit SSITH security features should be minimized. This capability may be achieved through an intermediate firmware layer, but use of the intermediate firmware is intended to be transparent to the application software programmer.

In addition to the PPAS impact, SSITH will also evaluate the ***scalability***, ***flexibility***, and ***adaptability*** of the security architectures developed in the program. ***Scalability*** will be needed to apply across a broad range of applications from small, ultra-low power systems to large, high-performance systems. ***Flexibility*** will be needed to ensure responsiveness of hardware security to evolving system threats. ***Adaptability*** will allow hardware systems to respond to detected attacks.

Out of Scope Technical Areas
The SSITH BAA will not focus on attacks that are not mediated through software access to the hardware. Although other areas of security are important, SSITH will focus on hardware vulnerabilities that are exploited through software to define achievable goals in a limited, but critical, part of the overall cybersecurity enterprise. Examples of out of scope topics are:

1. Development of physical elements of hardware security such as Physically Unclonable Functions (PUF) and Random Number Generators (RNG). Physical elements can be used as a part of a SSITH proposal, but SSITH will not fund their development.
2. Protection against hardware-only vulnerabilities such as EM side-channel attacks or insertion of hardware Trojans during design and/or fabrication.
3. Vulnerabilities that occur exclusively in the software domain, such as insecure interaction between software components or cross-site request forgeries.

C. Program Structure

This BAA addresses the challenges to develop hardware security architectures that are *scalable*, *flexible*, and *adaptable*. DARPA seeks proposals that demonstrate how these attributes are enabled through integrated circuit security *design architectures* and *design tools*. The goal of enabling *scalable*, *flexible*, and *adaptable* designs within design tool frameworks will be pursued concurrently in two Technical Areas across three phases with a total program period of performance of 39 months.

D. Technical Areas

This SSITH BAA is soliciting proposals in two technical areas:

Technical Area 1 (TA-1) will develop ***scalable***, ***flexible***, and ***adaptable*** integrated circuit security architectures that can be easily implemented in DoD and commercial SoCs.

Technical Area 2 (TA-2) will establish a methodology for evaluating the security provided by the architectures developed in TA-1.

Individual proposals shall address only one of the two technical areas; organizations wishing to propose to both technical areas must submit a separate proposal for each.

1. Technical Area 1: Novel hardware security architectures and design tool development

The focus of TA-1 is new hardware security approaches and architectures that will be used by DoD and commercial SoC designers to protect electronic systems against external software-assisted attacks. TA-1 is comprised of three key elements, 1) tasks, 2) characteristics, and 3) metrics, all of which are intended to be clearly represented and demonstrated throughout the program. Successful TA-1 proposers will illustrate the interdependency and evolution of key elements within each phase.

TA-1 Key elements:

1. Tasks:
    a. ***Security Architectures*:** develop and demonstrate one or more security architectures that can be used to protect electronics systems from software-assisted attacks that exploit the 7 CWE hardware vulnerability classes. TA-1 teams are requested to show how the security architecture will secure designs, and how it would be implemented.
    b. ***Design Tool Development:*** develop design tools required to implement the chosen security architectures in arbitrary circuit designs. The design tools may include methods or techniques which utilize new EDA software developments and/or modifications to existing EDA software that enable other design teams to utilize the security architecture to secure future circuit designs. Proposals should include details about how the design tools developed in TA-1 would insert security at the hardware level into circuit elements, circuit blocks and hardware architectures.
    c. ***Impact of security implementation****:* evaluate the impact of the security architecture implementation on key circuit metrics as described in section 3, and demonstrate the impact on circuit metrics through simulation and custom circuit emulation.

    **Note: Please refer to Table 2 for specific TA-1 tasks by phase.

2. Characteristics:
    a. ***Scalability*:** demonstrate that implementation of the security architecture enables scaling of security across a wide range of system parameters, such as power, performance, and complexity. Demonstrate that scalability will enable use of security architectures across a wide range of applications (small to large).
    b. ***Flexibility:*** demonstrate that the selected security architecture can be used to upgrade hardware to protect against newly found vulnerabilities without requiring redesign of the hardware.
    c. ***Adaptability:*** demonstrate that the selected security architecture can adapt system characteristics to respond to detected known attacks on the electronic system without reprogramming or firmware modification. Demonstrations will show the ability of the architecture to detect and adaptively respond to classes of attacks in an appropriate manner. For example, the security

architecture could detect a request for inappropriate permission access through an IO by lowering the IO transfer rate and restricting data exchange to known safe pathways.

3. Metrics:
    a. ***Security*:** demonstrate that selected security architectures effectively secure electronic systems against attacks on all seven (7) CWE hardware vulnerability classes described in Appendix 3. TA-1 teams are requested to address
        i. a theoretical evaluation of protection;
        ii. evaluation of the protection architecture against security metrics established by TA-2 performers; and
        iii. resistance of the security architecture against a 'red team' attack on the architecture as instantiated in hardware.
    b. ***Performance at power***: accurately quantify the *impact of implementing security on key circuit parameters* such as circuit performance, power, robustness, and reliability. TA-1 teams are requested to demonstrate the ability to trade-off these parameters against each other and with respect to metrics a (***security***) and c (***area/complexity***).

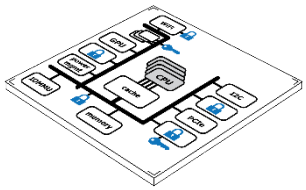
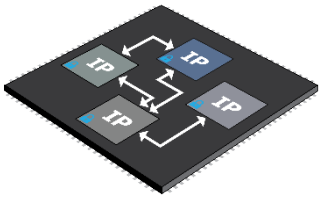
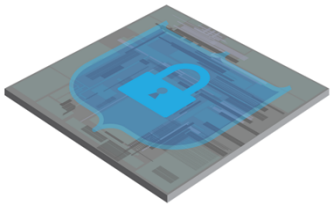
    c. ***Area/complexity***: accurately quantify the *impact of implementing security on circuit area and on design complexity*. TA-1 teams are requested to demonstrate the ability to trade-off these parameters against each other and with respect to metrics a (*security*) and b (*performance at power*).

    d. ***Software compatibility***: ensure that existing application software will run on hardware secured with SSITH and minimize the amount of software modifications required to implement all of the SSITH security features.

    *Note: Please refer to Table 2

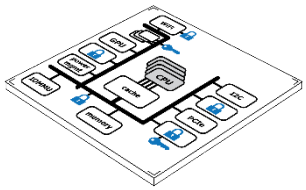
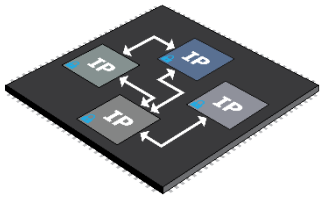
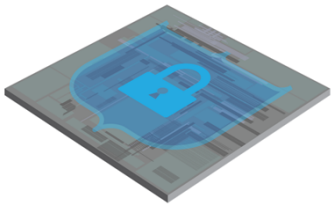
    for quantitative TA-1 metrics by phase.

Table 1. TA-1 Tasks by Phase

Phase 1	Phase 2	Phase 3
		
Security architectures 1. Prove feasibility of security architectures that provide protection against the seven CWE classes of hardware vulnerabilities.	Security architectures 1. Implement security architectures in circuit designs.	Security architectures 1. Implement security architectures in circuit designs.
Design tool development 2. Develop *alpha* design tools* that implement security architectures.	Design tool development 2. Develop *beta ** design tools* that implement security architectures. 3. Implement security architectures on the three GFE-provided FPGA designs using design tools.	Design tool development 2. Develop *distribution*** design tools* to implement security architectures. 3. Implement a second version of the security architectures on the three GFE-provided FPGA designs using design tools.
Impact of security on metrics 3. Establish, by simulation, impact of security architectures on PPASS: • Power/performance • Design area/complexity • Security • Software compatibility	Impact of security on metrics 4. Establish by simulation and FPGA demo, impact of security architecture on PPASS. 5. Support implementation of security architectures.	Impact of security on metrics 4. Establish, by and simulation and FPGA demo, impact of security architecture on PPASS. 5. Support implementation of security architectures .

*** Alpha: Usable by the developing team**
**** Beta: Usable by other design teams with significant interaction with the developing team**
***** Distribution: Sufficiently robust and documented for use by other design teams without support of the developing team**

Table 2. TA-1 Metrics by Phase

Phase 1	Phase 2	Phase 3
		
1. Provide 100% protection against at least **three (3)** CWE (reference) classes of the defined hardware vulnerabilities exploited by software attacks.	1. Provide 100% protection against at least **five (5)** CWE (reference) classes of the defined hardware vulnerabilities exploited by software attacks.	1. Provide 100% protection against all **seven (7)** CWE (reference) classes of the defined hardware vulnerabilities exploited by software attacks.
2. Prove security protection *against the three (3) CWE classes* through use of simulation and theoretical justification derived from performer-selected design.	2. Prove security protection *against the five (5) CWE classes* through red-team attack on the first pass FPGA instantiation of the three Government-provided GFE processor designs.	2. Prove security protection *against the seven (7) CWE classes* through red-team attack on the second pass FPGA instantiation of the three Government-provided GFE processor designs.
3. Provide quantitative simulation data indicating that improvement on system power, performance, and area (PPA) overhead meets Phase 1 metrics while maintaining software compatibility: -Performance impact < 20% -Power impact = 0% -Area impact < 50%	3. Provide quantitative simulation and FPGA data indicating that improvement on system power, performance, and area (PPA) overhead meets Phase 2 metrics while maintaining software compatibility: -Performance impact < 15% -Power impact = 0% -Area impact < 40%	3. Provide quantitative simulation and FPGA data indicating that improvement on system power, performance, and area (PPA) overhead meets Phase 3 metrics while maintaining software compatibility: -Performance impact < 10% -Power impact = 0% -Area impact < 30%
4. Provide theoretical or empirical evidence of the ability to respond to new hardware vulnerabilities without modifying hardware.	4. Demonstrate the ability to respond to new hardware vulnerabilities without modifying FPGA hardware.	4. Demonstrate the ability to respond to new hardware vulnerabilities without modifying FPGA hardware.

2. Technical Area 2: Security Evaluation Methodologies and Metrics

The focus of TA-2 is to develop a methodology and metrics by which to measure secure electronic systems. Specifically, TA-2 teams are intended to develop quantitative metrics required to evaluate trade-offs in security, performance, power, area and other standard circuit metrics. In addition, TA-2 teams are intended to establish a framework that enables representation of hardware/firmware security properties to overall system designers.

***Note: Please refer to Table 3 for specific TA-2 tasks by phase.

TA-2 is comprised of two key tasks that will evolve across the three phases of the program:

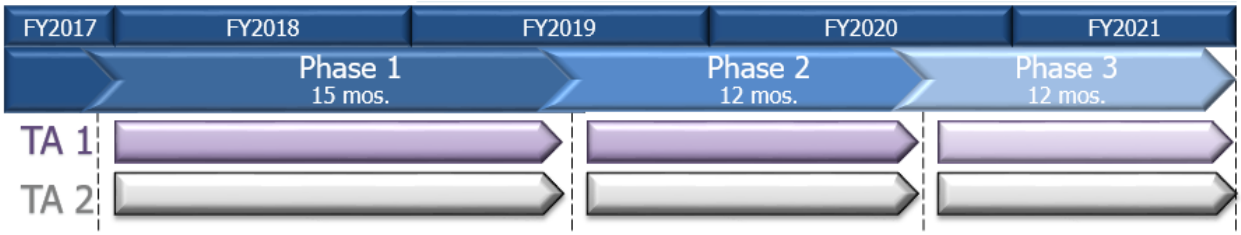
1. ***Definition of quantitative security metrics for hardware security*:** These metrics are intended to be measureable and enable trade-off decisions with respect to other circuit parameters such as performance, power, and area. The metrics are intended to correlate with both the attack vector (e.g., software, IO port) and the protection surface (e.g., software intrusion, IO intrusion).
2. ***Establishment of a framework for hardware/firmware security:*** This framework will permit overall evaluation of system security. The framework is intended to have a theoretical and/or empirical foundation and enable a common basis on which to communicate and evaluate security properties.

Table 3. TA-2 Tasks by Phase

Phase 1	Phase 2	Phase 3
1. Define initial quantitative metrics for the hardware/firmware security and coordinate use of these metrics to evaluate TA-1 performers.	1. Finalize the security metrics and support their use to drive engineering tradeoffs in the first version of the FPGA designs.	1. Formalize security metrics and support their use to drive engineering tradeoffs in the second version of the FPGA designs.
2. Establish an initial theoretical security representation framework.	2. Refine the security representation framework established in Phase 1 and support use of the framework by TA-1 teams to represent their hardware security architectures.	2. Collaborate with TA-1 design teams to represent their security properties in the established security representation framework.

E. Program Schedule

The SSITH program schedule comprises a 15-month base period (Phase 1) followed by two 12-month periods (Phases 2 and 3 respectively), for a total of 39 months, subject to the availability of funds.



Phase 1: Base Period (15 months)
TA-1: Demonstrate, through simulation, implementation of selected security architectures in integrated circuit designs to protect against **three (3)** of the seven (7) CWE hardware vulnerability classes, in compliance with Table 1: buffer errors, permissions/privileges, and information leakage. The demonstration circuit(s) will be chosen by performers to represent a broad range of DoD and/or commercial applications. TA-1 teams will develop alpha-level design tools to implement the security architectures and demonstrate use of those design tools to

implement the security architectures. Finally, in Phase 1, TA-1 teams will quantify the tradeoffs between security as implemented by their security architecture, and key circuit parameters such as performance, power, area, software compatibility, and complexity.

TA-2: Establish an initial set of quantitative metrics and coordinate use of the initial metrics to evaluate the results of TA-1 performers. TA-2 teams are expected to work with TA-1 performers to refine the metrics and facilitate the application of the metrics to TA-1 security architectures. TA-2 teams will also establish an initial theoretical framework for security representation.

Phase 2: Option 1 (12 months)
TA-1: Demonstrate, through implementation in an FPGA platform the ability of selected security architectures to protect against **five (5)** of the seven (7) CWE hardware vulnerability classes, in compliance with Table 1: buffer errors, permissions/privileges, information leakage, resource management, and crypto errors. Demonstration circuits will include three government-provided RISC-V processor designs spanning from a low-end to a high-end processor design. TA-1 teams will develop beta-level design tools to implement the security architectures, and demonstrate use of those design tools to implement security architectures on a FPGA platform. Using simulation and the FPGA platform, TA-1 teams will quantify trade-offs between security (as implemented by their security architecture), and key circuit parameters, such as performance, power, area, software compatibility, and complexity. Finally, TA-1 teams will establish an initial hardware representation of the selected security architecture based on a security representation framework defined by TA-2.

TA-2: Finalize quantitative metrics to be used by TA-1 design teams as engineering parameters to drive appropriate tradeoffs in circuit design. The final set of security metrics from this phase will be used to evaluate program results. Finally, TA-2 teams will refine the initial security representation framework and collaborate with TA-1 performers to represent TA-1 security architectures in the security representation framework.

Phase 3: Option 2 (12 months)
TA-1: Demonstrate, through implementation in a second version of the FPGA designs, the ability of selected security architectures to protect against **all seven (7)** of the CWE hardware vulnerability classes, in compliance with Table 1. The demonstration circuits will include three (3) government-provided RISC-V processor designs spanning from a low-end to a high-end processor design. TA-1 teams will develop production-level design tools to implement the security architectures and demonstrate use of those design tools to implement their security architectures. Using simulation and the second version of the FPGA designs , TA-1 teams will quantify the trade-offs between security as implemented by their security architecture, and key circuit parameters such as performance, power, area, software compatibility, and complexity. Finally, TA-1 teams will establish a final hardware representation of the selected security architecture based on the security representation framework defined by TA-2.

TA-2: Formalize security metrics, continue to support use of these metrics by TA-1 design teams, and disseminate the security metrics to the broader security community.

F. Deliverables

Table 4.1. TA-1 Deliverables by Phase

Phase 1	Phase 2	Phase 3
1. Simulation data indicating the impact of security architectures on circuit performance, power, area, software compatibility, and design complexity.	1. Simulation and first version FPGA data indicating the impact of security architectures on circuit performance, power, area, software compatibility, and design complexity.	1. Simulation and second version FPGA data indicating the impact of security architectures on circuit performance, power, area, software compatibility, and design complexity.
2. Alpha-level design tools that implement selected security architectures.	*2. Beta-level design tools* that implement selected security architectures.	*2. Production-level design tools* that implement selected security architectures.
3. Quarterly and end of phase technical reports and monthly financial reports.	3. First pass bitstream and RTL descriptions of the GFE-provided designs that include implementation of the selected security architecture(s).	3. Final bitstream and RTL descriptions of the GFE-provided designs that include implementation of the selected security architecture(s).
	4. Quarterly and end of phase technical reports and monthly financial reports.	4. Quarterly and end of program technical reports and monthly financial reports.

Table 4.2. TA-2 Deliverables by Phase

Phase 1	Phase 2	Phase 3
1. Initial set of quantitative metrics.	1. Final set of quantitative metrics.	1. Quarterly and end of phase technical reports and monthly financial reports.
2. Initial security representation framework.	2. Final security representation framework.	
3. Quarterly and end of phase technical reports and monthly financial reports.	3. Quarterly and end of phase technical reports and monthly financial reports.	

G. Government Furnished Property/Information

Proposers to TA-1 may expect the following government furnished property to be made available at the beginning of Phase 2:

1. An FPGA board with IOs and 2X the capacity required to implement the most complex RISC-V baseline circuit. The FPGA board will be mounted in a chassis containing the FPGA board and accessible IOs.
2. RTL and FPGA bitstream for three different sizes of RISC-V processor designs:

a. A small, reduced-feature version of the Rocket processor,
b. A full-featured, single threaded version of the Rocket processor, and
c. A full-featured, multi-threaded, out of order execution RISC-V processor.

3. Versions of an Operating System that can be run on each of the three processors.

II. Award Information

A. General Award Information

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

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

Awards under this BAA will be made to proposers on the basis of the evaluation criteria listed below (see section labeled "Application Review Information," Sec. V.), and program balance to provide overall value to the Government. The Government reserves the right to request any additional, necessary documentation once it makes the award instrument determination. Such additional information may include but is not limited to Representations and Certifications (see Section VI.B.2., "Representations and Certifications"). The Government reserves the right to remove proposers from award consideration should the parties fail to reach agreement on award terms, conditions and cost/price within a reasonable time or the proposer fails to timely provide requested additional information. Proposals identified for negotiation may result in a procurement contract or other transaction, depending upon the nature of the work proposed, and other factors.

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

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 proposers not intending to perform fundamental research or the proposed research may present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Based on the nature of the performer and the nature of the work, the Government anticipates that some awards will include restrictions on the resultant research that will require the awardee to seek DARPA permission before publishing any information or results relative to the program.

Proposers should indicate in their proposal whether they believe the scope of the research included in their proposal is fundamental or not. While proposers should clearly explain the intended results of their research, the Government shall have sole discretion to 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 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

III. Eligibility Information

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

A. Eligible Applicants

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. Non-U.S. Organizations and/or Individuals

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

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

D. Other Eligibility Criteria

1. Collaborative Efforts

Collaborative efforts/teaming are encouraged as appropriate to meet the goals of the program.

2. Ability to Receive Awards in Multiple Technical Areas – Conflicts of Interest (COIs)

While proposers may submit proposals for both Technical Areas 1 and 2, proposers may not be selected for both Technical Area 1 and for Technical Area 2, whether as a prime, subcontractor, or in any other capacity, from an organizational to an individual level.

E. Associate Contractor Agreement Clause

This same or similar clause will be included in all awards against HR001117S0023:

> (a) It is recognized that success of the SSITH research effort depends in part upon the open exchange of information between the various Associate Contractors involved in the effort. This clause is intended to insure 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 clause, 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 SSITH 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 SSITH 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 clause, including this paragraph (e).

Note: It is intended that ACA's be established, after selections and prior to contract award, between each TA-1 and TA-2 performer.

IV. Application and Submission Information

PROPOSERS ARE CAUTIONED THAT EVALUATION RATINGS MAY BE LOWERED AND/OR PROPOSALS REJECTED IF PROPOSAL PREPARATION (PROPOSAL FORMAT, CONTENT, ETC.) AND/OR SUBMITTAL INSTRUCTIONS ARE NOT FOLLOWED.

A. Address to Request Application Package

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

B. Content and Form of Application Submission

1. Full Proposal Format

All full proposals must be in the format given below. Proposals shall consist of two volumes: Volume I – Technical and Management Proposal (3 sections), and Volume II – Cost Proposal (4 sections). The submission of other supporting materials along with the proposals is strongly discouraged and will not be considered for review. All pages shall be printed on 8-1/2 by 11 inch

paper with type not smaller than 12 point. Smaller font may be used for figures, tables and charts. The page limitation for full proposals includes all figures, tables, and charts.

Section II of Volume I, Technical and Management Proposal, shall not exceed 30 pages for a proposal responding to TA-1, or 20 pages for a proposal responding to TA-2. Individual proposals should address one of the two technical areas; organizations wishing to propose to both technical areas must submit a separate proposal for each. All full proposals must be written in English.

A summary slide of the proposed effort, in PowerPoint format, should be submitted with the proposal. A template slide is provided as Attachment 2 to the BAA. Submit this PowerPoint file in addition to Volumes I and II of your full proposal. This summary slide does not count towards the total page count.

a. Volume I, Technical and Management Proposal

Section I. Administrative

A. Cover sheet to include:

(1) BAA number (HR001117S0023);
(2) Technical area;
(3) Lead Organization submitting proposal;
(4) Type of organization, selected among the following categories:
Large Organization, Small Disadvantaged Organization, Other Small Organization, HBCU, MI, Other Educational, Other Nonprofit;
(5) Proposer's internal reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;
(8) Technical point of contact to include:
Salutation, last name, first name, street address, city, state, zip code (+4), telephone, fax (if available), electronic mail;
(9) Administrative point of contact to include:
Salutation, last name, first name, street address, city, state, zip code (+4), telephone, fax (if available), electronic mail;
(10) Total funds requested from DARPA, and the amount of cost share (if any); AND
(11) Date proposal was submitted.

B. Official transmittal letter.

The transmittal letter should identify the BAA number, the proposal by name, and the proposal reference number (if any), and should be signed by an individual from the prime organization who is authorized to submit proposals to the Government.

Section II. Detailed Proposal Information

A. Executive Summary
A one-page executive summary outlining the proposed effort. The executive summary must contain:

1. A high-level overview of the proposed work;
2. Metrics used to define success;
3. Milestones (both DARPA-mandated and proposed-defined);
4. Operational scenarios relevant to the proposed approach;
5. Innovations made by the proposed work; AND
6. The cost and duration of each phase.

B. Technical Approach
A detailed description of the technical approach, technical rationale, and constructive plan for accomplishment of technical goals in support of the innovative claims and deliverables. This section is the centerpiece of the proposal and should succinctly describe the uniqueness and benefits of the proposed approach. Proposers must include adequate detail and justification for any performer-defined metrics and goals. In addition, a detailed analysis of how the proposed approach will meet both the DARPA and performer defined metrics must be provided.

For TA-1 a clear description of how the proposed security architecture would exhibit the required characteristics (scalability, flexibility, and adaptability) should be provided. It is also critical for proposers to describe how they will evaluate the tradeoff between power, performance, area, software compatibility. A clear plan for design tool development should also be provided that indicates the level of new tools that would be developed as well as the extent to which existing design tools would be utilized.

For TA-2 a clear description of how the proposer will interact with TA-1 performers should be provided. The description should include how a two-way exchange of information and ideas will be fostered and utilized. Proposers should also indicate how they will connect the hardware and software communities through the means of security representations.

C. State-of-the-Art Comparison
Comparison between the proposed work and the state-of-the-art, along with a general discussion of other research in this area. This section should be no more than 1 page long.

D. Statement of Work
Statement of Work (SOW) - In plain English, clearly define the technical area, phases, tasks/subtasks to be performed, their durations, and dependencies among them. The page length for the SOW will be dependent on the amount of the effort. The SOW must not include proprietary information. For each task/subtask, provide:

1. A general description of the objective (for each defined task/activity);
2. A detailed description of the approach to be taken to accomplish each defined task/activity;
3. Identification of the primary organization responsible for task execution (prime, sub, team member, by name, etc.);

4. The completion criteria for each task/activity - a product, event or milestone that defines its completion;
5. A definition of all deliverables (data, reports, design files, hardware, etc.) to be provided to the Government in support of the proposed research tasks/activities; AND
6. Clear identification of any tasks/subtasks (prime or subcontracted) that will be accomplished on-campus at a university.

Note: Each Phase, each Technical Area and each Option of the program must be separately defined in the SOW.

E. Deliverables
For all technical areas, expected deliverables include quarterly technical and financial update reports and a final report at the end of each phase. Include in this section all proprietary claims to the results, prototypes, intellectual property, or systems supporting and/or necessary for the use of the research, results, and/or prototype. If there are no proprietary claims, this should be stated. For forms to be completed regarding intellectual property, see Section VIII. There will be no page limit for the listed forms.

F. Risk Mitigation Plan
Plan detailing risks and proposed activities to mitigate or respond to these risks. The risk plan should include a metric showing the probability of the risk occurring and another metric to capture the impact to the program. The impact of risks should be tied to the overall program objectives. This section should be no more than 1 page long.

G. Schedule and Measureable Milestones
Schedule and measurable milestones for the proposed research. Measurable milestones should capture key development points in tasks and should be clearly articulated and defined in time relative to start of effort. Where the effort consists of multiple portions which could reasonably be partitioned for purposes of funding, these should be identified as options. Additionally, proposals should clearly explain the technical approach(es) that will be employed to meet or exceed each program metric and provide ample justification as to why the approach(es) is/are feasible. The milestones must not include proprietary information. This section should be no more than 2 pages long.

H. Teaming Plan
A clearly defined organization chart for the program team which includes, as applicable: (1) the programmatic relationship of team member, (2) the unique capabilities of team members; (3) the task of responsibilities of team members, (4) the teaming strategy among the team members, and (5) the key personnel along with the amount of effort to be expended by each person during each year. Formal teaming agreements can be added to the end of this section titled “Teaming Appendix” and will not count against the total number pages for this section.

I. Previous Accomplishments
Discussion of the proposer’s previous accomplishments and work in closely related research areas. This section should be no more than 1 page long.

J. Technical Transfer
Description of the results, products, transferable technology, and expected technology transfer path. This section should also describe the plans and capability to accomplish technology transition and commercialization. This should also address mitigation of life-cycle and sustainment risks associated with transitioning intellectual property for U.S. military applications, if applicable. This section should be no more than 1 page long.

K. Facilities
Description of the differentiating facilities and capabilities that would be used for the proposed effort. This section should be no more than 1 page long.

Section III. Additional Information

Information in this section may include a brief bibliography of relevant technical papers and research notes (published and unpublished) which document the technical ideas upon which the proposal is based. Copies of not more than three (3) relevant papers may be included in the submission.

b. Volume II, Cost Proposal

All proposers, including FFRDCs and Government laboratories, must submit the following:

Section I. Administrative

Cover sheet to include:

(1) BAA number (HR001117S0023);
(2) Technical area;
(3) Lead Organization submitting proposal;
(4) Type of organization, selected among the following categories:
Large Organization, Small Disadvantaged Organization, Other Small Organization, HBCU, MI, Other Educational, Other Nonprofit;
(5) Proposer's internal reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;
(8) Technical point of contact to include:
Salutation, last name, first name, street address, city, state, zip code (+4), telephone, fax (if available), electronic mail (if available);
(9) Administrative point of contact to include:
Salutation, last name, first name, street address, city, state, zip code (+4), telephone, fax (if available), and electronic mail (if available);
(10) Award instrument requested:
Cost-Plus-Fixed Fee (CPFF), Cost-contract—no fee, cost sharing contract—no fee, or other type of procurement contract (*specify*) or Other Transaction;
(11) Place(s) and period(s) of performance;

(12) Total proposed cost separated by basic award and option(s), if any, by government fiscal year;
(13) Name, address, and telephone number of the proposer's cognizant Defense Contract Management Agency (DCMA) administration office (*if known)*;
(14) Name, address, and telephone number of the proposer's cognizant Defense Contract Audit Agency (DCAA) audit office (*if known*);
(15) Date proposal was prepared;
(16) DUNS number;
(17) TIN number;
(18) CAGE Code;
(19) Subcontractor Information;
(20) Proposal validity period; AND
(21) Any Forward Pricing Rate Agreement, other such approved rate information, or such documentation that may assist in expediting negotiations (if available).

Attachment 1, the Cost Volume Proposer Checklist, must be included with the coversheet of the Cost Proposal.

Section II. Detailed Cost Information (Prime and Subcontractors)

The proposers,' to include eligible FFRDCs,' cost volume shall provide cost and pricing information (See Note 1), or other than cost or pricing information if the total price is under the referenced threshold, in sufficient detail to substantiate the program price proposed (e.g., realism and reasonableness). In doing so, the proposer shall provide, **for both the prime and each subcontractor**, a "Summary Cost Breakdown" by technical area, phase and performer fiscal year, and a "Detailed Cost Breakdown" by phase, technical task/sub-task, and month for each technical area. The breakdown/s shall include, at a minimum, the following major cost items along with associated backup documentation:

Total program cost broken down by major cost items:

A. Direct Labor
A breakout clearly identifying the individual labor categories with associated labor hours and direct labor rates, as well as a detailed Basis-of-Estimate (BOE) narrative description of the methods used to estimate labor costs;

B. Indirect Costs
Including Fringe Benefits, Overhead, General and Administrative Expense, Cost of Money, Fee, etc. (must show base amount and rate);

C. Travel
Provide the purpose of the trip, number of trips, number of days per trip, departure and arrival destinations, number of people, etc.;

D. Other Direct Costs
Itemized with costs; back-up documentation is to be submitted to support proposed costs;

E. Material/Equipment

(i) For IT and equipment purchases, include a letter stating why the proposer cannot provide the requested resources from its own funding.

(ii) A priced Bill-of-Material (BOM) clearly identifying, for each item proposed, the quantity, unit price, the source of the unit price (i.e., vendor quote, engineering estimate, etc.), the type of property (i.e., material, equipment, special test equipment, information technology, etc.), and a cross-reference to the Statement of Work (SOW) task/s that require the item/s. At time of proposal submission, any item with a unit price that exceeds $1,000 must be supported with basis-of-estimate (BOE) documentation such as a copy of catalog price lists, vendor quotes or a detailed written engineering estimate (additional documentation may be required during negotiations, if selected).

(iii) If seeking a procurement contract and items of Contractor Acquired Property are proposed, exclusive of material, the proposer shall clearly demonstrate that the inclusion of such items as Government Property is in keeping with the requirements of FAR Part 45.102. In accordance with FAR 35.014, "Government property and title," it is the Government's intent that title to all equipment purchased with funds available for research under any resulting contract will vest in the acquiring nonprofit institution (e.g., Nonprofit Institutions of Higher Education and Nonprofit Organizations whose primary purpose is the conduct of scientific research) upon acquisition without further obligation to the Government. Any such equipment shall be used for the conduct of basic and applied scientific research. The above transfer of title to all equipment purchased with funds available for research under any resulting contract is not allowable when the acquiring entity is a for-profit organization; however, such organizations can, in accordance with FAR 52.245-1(j), be given priority to acquire such property at its full acquisition cost.

F. Consultants

If consultants are to be used, proposer must provide a copy of the consultant's proposed SOW as well as a signed consultant agreement or other document which verifies the proposed loaded daily / hourly rate and any other proposed consultant costs (e.g. travel);

G. Subcontracts

Itemization of all subcontracts. Additionally, the prime contractor is responsible for compiling and providing, as part of its proposal submission to the Government, subcontractor proposals prepared at the same level of detail as that required by the prime. Subcontractor proposals include Interdivisional Work Transfer Agreements (ITWA) or similar arrangements. If seeking a procurement contract, the prime contractor shall provide a cost reasonableness analysis of all proposed subcontractor costs/prices. Such analysis shall indicate the extent to which the prime contractor has negotiated subcontract costs/prices and whether any such subcontracts are to be placed on a sole-source basis.

All proprietary subcontractor proposal documentation (fully disclosed subcontract proposal), prepared at the same level of detail as that required of the prime, which cannot be uploaded to the DARPA BAA website (https://baa.darpa.mil, BAAT) as part of the proposer's submission, 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 organization. This does not relieve the proposer from the requirement to include, as part of their submission (via BAAT), subcontract proposals that do not include proprietary pricing information (rates, factors, etc.).

A Rough Order of Magnitude (ROM), or similar budgetary estimate, **is not considered a fully qualified subcontract cost proposal submission**. Inclusion of a ROM, or similar budgetary estimate, may result in the full proposal being deemed non-compliant or evaluation ratings may be lowered;

H. Cost-Sharing
The source, nature, and amount of any industry cost-sharing; AND

I. Fundamental Research
Written justification required per Section II.B, "Fundamental Research," pertaining to prime and/or subcontracted effort being considered Contracted Fundamental Research.

Note 1:
(a) "Cost or Pricing Data" as defined in FAR 15.403-4 shall be required if the proposer is seeking a procurement contract per the referenced threshold, unless the proposer requests and is granted an exception from the requirement to submit cost or pricing data. Per DFARS 215.408(5), DFARS 252.215-7009, Proposal Adequacy Checklist, applies to all proposers/proposals seeking a FAR-based award (contract).
(b) In accordance with DFARS 15.403-1(4)(D), DoD has waived cost or pricing data requirements for nonprofit organizations (including educational institutions) on cost-reimbursement-no-fee contracts. In such instances where the waiver stipulated at DFARs 15.403-1(4)(D) applies, proposers shall submit information other than cost or pricing data to the extent necessary for the Government to determine price reasonableness and cost realism; and cost or pricing data from subcontractors that are not nonprofit organizations when the subcontractor's proposal exceeds the cost and pricing data threshold at FAR 15.403-4(a)(1).
(c) Per Section 873 of the FY2016 National Defense Authorization Act (Pub L. 114-92), "Pilot Program For Streamlining Awards For Innovative Technology Projects," small businesses and nontraditional defense contractors (as defined therein) are alleviated from submission of certified cost and pricing data for new contract awards valued at less than $7,500,000. In such instances where this "waiver" applies, proposers seeking a FAR-based contract shall submit information other than certified cost or pricing data to the extent necessary for the Government to determine price reasonableness and cost realism; and certified cost or pricing data from subcontractors that are not small businesses or nontraditional defense contractors when such subcontract proposals exceed the cost and pricing data threshold at FAR 15.403-4(a)(1).
(d) "Cost or pricing data" are not required if the proposer proposes an award instrument other than a procurement contract (i.e., other transaction).

Note 2:
Proposers are strongly encouraged to provide the aforementioned cost breakdown as an editable MS Excel spreadsheet, inclusive of calculations formulae, with tabs (material, travel, ODC's) provided as necessary. The Government also requests and recommends that the Cost Proposal include MS Excel file(s) that provide traceability between the Bases of Estimate (BOEs) and the

proposed costs across all elements and phases. This includes the calculations and adjustments that are utilized to generate the Summary Costs from the source labor hours, labor costs, material costs, etc. input data. It is requested that the costs and Subcontractor proposals be readily traceable to the Prime Cost Proposal in the provided MS Excel file(s) – although this is not a requirement, providing information in this manner will assist the Government in understanding what is being proposed both technically and in terms of cost realism. NOTE: If the PDF submission differs from the Excel submission, the PDF will take precedence.

Section III. Other Transaction Request, if applicable

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

- Milestone description
- Completion criteria
- Due date
- Payment/funding schedule (to include, if cost share is proposes, awardee and Government share amounts)

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

Section IV. Other Cost Information

Where the effort consists of multiple portions which could reasonably be partitioned for purposes of funding, these should be identified as options with separate cost estimates.

The cost proposal should include identification of pricing assumptions of which may require incorporation into the resulting award instrument (i.e., use of Government Furnished Property/Facilities/Information, access to Government Subject Matter Experts, etc.).

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

Cost proposals submitted by FFRDC's (prime or subcontractor) will be forwarded, if selected for negotiation, to their sponsoring organization contracting officer for review to confirm that all required forward pricing rates and factors have been used.

2. 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 with a label such as "Proprietary" or "Company Proprietary." Note, "Confidential" is a classification marking used to control the dissemination of U.S. Government

National Security Information as dictated in Executive Order 13526 and should not be used to identify proprietary business information.

3. Security Information

a. Unclassified Submissions

DARPA anticipates that submissions received under this BAA will be unclassified. However, should a proposer wish to submit classified information, an *unclassified* email must be sent to the BAA mailbox notifying the Technical Office PSO of the submission and the below guidance must be followed.

Security classification guidance and direction via a Security Classification Guide (SCG) and/or DD Form 254, "DoD Contract Security Classification Specification," will not be provided at this time. If a determination is made that the award instrument may result in access to classified information, a SCG and/or DD Form 254 will be issued by DARPA and attached as part of the award.

b. Classified Submissions

Classified submissions shall be transmitted in accordance with the following guidance. Additional information on the subjects discussed in this section may be found at http://www.dss.mil/.

If a submission contains Classified National Security Information as defined by Executive Order 13526, the information must be appropriately and conspicuously marked with the proposed classification level and declassification date. Similarly, when the classification of a submission is in question, the submission must be appropriately and conspicuously marked with the proposed classification level and declassification date. Submissions requiring DARPA to make a final classification determination shall be marked as follows:

> "CLASSIFICATION DETERMINATION PENDING. Protect as though classified _____ *(insert the recommended classification level, e.g., Top Secret, Secret or Confidential).*"

NOTE: Classified submissions must indicate the classification level of not only the submitted materials, but also the classification level of the anticipated award.

Proposers submitting classified information must have, or be able to obtain prior to contract award, cognizant security agency approved facilities, information systems, and appropriately cleared/eligible personnel to perform at the classification level proposed. All proposer personnel performing Information Assurance (IA)/Cybersecurity related duties on classified Information Systems shall meet the requirements set forth in DoD Manual 8570.01-M (Information Assurance Workforce Improvement Program).

When a proposal includes a classified portion, and when able according to security guidelines, we ask that proposers send an e-mail to HR001117S0023@darpa.mil as notification that there is

a classified portion to the proposal. When sending the classified portion via mail according to the instructions, proposers should submit six (6) hard copies of the classified portion of their proposal and two (2) CD-ROMs containing the classified portion of the proposal as a single searchable Adobe PDF file. Please ensure that all CDs are well-marked. Each copy of the classified portion must be clearly labeled with HR001117S0023, proposer organization, proposal title (short title recommended), and Copy _ of _.

Proposers choosing to submit classified information from other collateral classified sources (i.e., sources other than DARPA) must ensure (1) they have permission from an authorized individual at the cognizant Government agency (e.g., Contracting Officer, Program Manager); (2) the proposal is marked in accordance with the source Security Classification Guide (SCG) from which the material is derived; and (3) the source SCG is submitted along with the proposal.

Confidential and Secret Information
Use transmission, classification, handling, and marking guidance provided by previously issued SCGs, the DoD Information Security Manual (DoDM 5200.01, Volumes 1 - 4), and the National Industrial Security Program Operating Manual, including the Supplement Revision 1, (DoD 5220.22-M and DoD 5200.22-M Sup. 1) when submitting Confidential and/or Secret classified information.

Confidential and Secret classified information may be submitted via ONE of the two following methods:

- Hand-carried by an appropriately cleared and authorized courier to the DARPA CDR. Prior to traveling, the courier shall contact the DARPA Classified Document Registry (CDR) at 703-526-4052 to coordinate arrival and delivery.
  OR
- Mailed via U.S. Postal Service (USPS) Registered Mail or USPS Express Mail. All classified information will be enclosed in opaque inner and outer covers and double-wrapped. The inner envelope shall be sealed and plainly marked with the assigned classification and addresses of both sender and addressee.

  The inner envelope shall be addressed to:

  Defense Advanced Research Projects Agency
  ATTN: Program Security Officer, MTO
  Reference: HR001117S0023
  675 North Randolph Street
  Arlington, VA 22203-2114

  The outer envelope shall be sealed with no identification as to the classification of its contents and addressed to:

  Defense Advanced Research Projects Agency
  Security & Intelligence Directorate, Attn: CDR
  675 North Randolph Street

Arlington, VA 22203-2114

Top Secret Information
Use classification, handling, and marking guidance provided by previously issued SCGs, the DoD Information Security Manual (DoDM 5200.01, Volumes 1 - 4), and the National Industrial Security Program Operating Manual, including the Supplement Revision 1, (DoD 5220.22-M and DoD 5200.22-M Sup. 1). Top Secret information must be hand-carried by an appropriately cleared and authorized courier to the DARPA CDR. Prior to traveling, the courier shall contact the DARPA CDR at 703-526-4052 to coordinate arrival and delivery.

Sensitive Compartmented Information (SCI)
SCI must be marked, managed and transmitted in accordance with DoDM 5105.21 Volumes 1 - 3. Questions regarding the transmission of SCI may be sent to the DARPA Technical Office PSO via the BAA mailbox or by contacting the DARPA Special Security Officer (SSO) at 703-812-1970.

Successful proposers may be sponsored by DARPA for access to SCI. Sponsorship must be aligned to an existing DD Form 254 where SCI has been authorized. Questions regarding SCI sponsorship should be directed to the DARPA Personnel Security Office at 703-526-4543.

Special Access Program (SAP) Information
SAP information must be marked in accordance with DoDM 5205.07 Volume 4 and transmitted by specifically approved methods which will be provided by the Technical Office PSO or their staff.

Proposers choosing to submit SAP information from an agency other than DARPA are required to provide the DARPA Technical Office Program Security Officer (PSO) written permission from the source material's cognizant Special Access Program Control Officer (SAPCO) or designated representative. For clarification regarding this process, contact the DARPA Technical Office PSO via the BAA mailbox or the DARPA SAPCO at 703-526-4102.

Additional SAP security requirements regarding facility accreditations, information security, personnel security, physical security, operations security, test security, classified transportation plans, and program protection planning may be specified in the DD Form 254.

NOTE: prior to drafting the submission, if use of SAP Information Systems is to be proposed, proposers must first obtain an Authorization-to-Operate from the DARPA Technical Office PSO (or other applicable DARPA Authorization Official) using the Risk Management Framework (RMF) process outlined in the Joint Special Access Program (SAP) Implementation Guide (JSIG), Revision 3, dated October 9, 2013 (or successor document).

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

Unless a proposer is performing strictly fundamental research, all proposers receiving FAR-based Procurement Contracts under this BAA shall be compliant with the following:

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, or as authorized by the Contracting Officer, not later than December 31, 2017.

5.

6. Human Research Subjects/Animal Use

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

7. Approved Cost Accounting System Documentation

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

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

All electronic and information technology acquired or created through this BAA must satisfy the accessibility requirements of Section 508 of the Rehabilitation Act (29 U.S.C § 794d)/FAR 39.2.

9. Small Business Subcontracting Plan

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

10. Intellectual Property

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

a. For Procurement Contracts

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

Technical Data Computer Software To be Furnished With Restrictions	Summary of Intended Use in the Conduct of the Research	Basis for Assertion	Asserted Rights Category	Name of Person Asserting Restrictions
(LIST)	(NARRATIVE)	(LIST)	(LIST)	(LIST)

b. For All Non-Procurement Contracts

Proposers responding to this BAA requesting a Technology Investment Agreement or Other Transaction for Prototypes shall follow the applicable rules and regulations governing these various award instruments, but, in all cases, should appropriately identify any potential restrictions on the Government's use of any Intellectual Property contemplated under the award instrument in question. This includes both Noncommercial Items and Commercial Items. Proposers are encouraged use a format similar to that described in Paragraph a. above. If no restrictions are intended, then the proposer should state "NONE."

11. Patents

Include documentation proving your ownership of or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) that will be utilized under your proposal for the DARPA program. If a patent application has been filed for an invention that your proposal utilizes, but the application has not yet been made publicly available and contains proprietary information, you may provide only the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and a summary of the patent title, together with either: (1) a representation that you own the invention, or (2) proof of possession of appropriate licensing rights in the invention.

12. 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 www.darpa.mil/work-with-us/additional-baa for further information.

13. Funding Restrictions

Preaward costs will not be reimbursed unless a preaward cost agreement is negotiated prior to award.

C. Submission Information

DARPA will acknowledge receipt of all submissions and assign an identifying control number that should be used in all further correspondence regarding the submission. DARPA intends to use electronic mail correspondence regarding HR001117S0023. **Submissions may not be submitted by fax or e-mail; any so sent will be disregarded.**

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

All administrative correspondence and questions on this solicitation, including requests for clarifying information on how to submit a full proposal to this BAA should be directed to HR001117S0023@darpa.mil. DARPA intends to use electronic mail for correspondence regarding HR001117S0023. Proposals may not be submitted by fax or e-mail; any so sent will be disregarded. DARPA encourages use of the Internet for retrieving the BAA and any other related information that may subsequently be provided.

1. Submission Dates and Times

a. Full Proposal Date

Full proposals must be submitted to DARPA/MTO on or before 1:00 PM, Eastern Time, June 5, 2017 in order to be considered during the single round of selections. Proposals received after this deadline will not be reviewed.

b. Frequently Asked Questions (FAQ)

DARPA will post a consolidated Question and Answer (FAQ) document on a regular basis. To access the posting go to: http://www.darpa.mil/work-with-us/opportunities. Under the HR001117S0023 summary will be a link to the FAQ. Submit your question/s by e-mail to HR001117S0023@darpa.mil. In order to receive a response sufficiently in advance of the proposal due date, send your question/s on or before 1:00 PM, Eastern Time, May 22, 2017.

2. Proposal Submission Information

The typical proposal should express a consolidated effort in support of one or more related technical concepts or ideas. Disjointed efforts should not be included into a single proposal. Proposals not meeting the format described in the BAA may not be reviewed. Proposals requesting grants or other assistance instruments will not be accepted.

a. For Proposers Requesting Contracts or Other Transaction Agreements

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

All unclassified full proposals submitted electronically through the DARPA BAA website must be uploaded as zip files (.zip or .zipx extension). The final zip file should not exceed 50 MB in size. Only one zip file will be accepted per submission and submissions not uploaded as zip files will be rejected by DARPA.

NOTE: YOU MUST CLICK THE 'FINALIZE FULL PROPOSAL' BUTTON AT THE BOTTOM OF THE CREATE FULL PROPOSAL PAGE. FAILURE TO DO SO WILL RESULT IN YOUR PROPOSAL NOT BEING OFFICIALLY SUBMITTED TO THIS BAA AND THEREFORE NOT BEING REVIEWED.

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

Please note that the DoD-issued certificate associated with the BAA website is not recognized by all commercial certificate authorities, resulting in untrusted connection errors/messages. You can either bypass the warning (possibly by adding https://baa.darpa.mil to your listed of trusted sites, or darpa.mil as a trusted domain), or visit DISA's site to download the Root Certificate Authority (CA): http://dodpki.c3pki.chamb.disa.mil/rootca.html.

Technical support for DARPA's BAA Website may be reached at BAAT_Support@darpa.mil, and is typically available during regular business hours (9:00 AM - 5:00 PM EST, Monday - Friday).

b. Classified Submission Information

See Section IV.B.4, "Security Information," for guidance on submitting classified proposals.

3. Other Submission Requirements

Not applicable.

V. Application Review Information

A. Evaluation Criteria

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

1. Overall Scientific and Technical Merit

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

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

2. Potential Contribution and Relevance to the DARPA Mission

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

3. Plans and Capability to Accomplish Technology Transition

The proposer clearly demonstrates its capability to transition the technology to the research, industrial, and/or operational military communities in such a way as to enhance U.S. defense. In addition, the evaluation will take into consideration the extent to which the proposed intellectual property (IP) rights structure will potentially impact the Government's ability to transition the technology.

4. Proposer's Capabilities and/or Related Experience

The proposer's prior experience in similar efforts clearly demonstrates an ability to deliver products that meet the proposed technical performance within the proposed budget and schedule. The proposed team has the expertise to manage the cost and schedule. Similar efforts completed/ongoing by the proposer in this area are fully described including identification of other Government sponsors.

5. Realism of Proposed Costs and Schedule

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

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

B. Review and Selection Process

1. Review Process

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

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

Award(s) will be made to proposers whose proposals are determined to be the most advantageous to the Government, all factors considered, including the potential contributions of the proposed work to the overall research program and the availability of funding for the effort.

It is the policy of DARPA to ensure impartial, equitable, comprehensive proposal evaluations based on the evaluation criteria listed above and to select the source (or sources) whose offer meets the Government's technical, policy, and programmatic goals. Pursuant to FAR 35.016, the primary basis for selecting proposals for acceptance shall be technical, importance to agency programs, and fund availability. In order to provide the desired evaluation, qualified Government personnel will conduct reviews and (if necessary) convene panels of experts in the appropriate areas.

2. Handling of Source Selection Information

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

Subject to the restrictions set forth in FAR 37.203(d), input on technical aspects of the proposals may be solicited by DARPA from non-Government consultants/experts who are strictly bound by the appropriate non-disclosure requirements.

3. Federal Awardee Performance and Integrity Information (FAPIIS)

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

VI. Award Administration Information

A. Selection Notices

1. Proposals

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

B. Administrative and National Policy Requirements

1. Meeting and Travel Requirements

All key participants are required to attend the program kickoff meeting. Performers should also anticipate regular program-wide PI Meetings and periodic site visits at the Program Manager's discretion.

2. 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.

3. 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.

4. 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 www.darpa.mil/work-with-us/additional-baa.
.

C. Reporting

The number and types of reports will be specified in the award document, but will include as a minimum quarterly technical and monthly financial status reports. The reports shall be prepared and submitted in accordance with the procedures contained in the award document and mutually agreed on before award. Reports and briefing material will also be required as appropriate to document progress in accomplishing program metrics. A Final Report that summarizes the project and tasks will be required at the conclusion of the performance period for the award, notwithstanding the fact that the research may be continued under a follow-on vehicle.

D. Electronic Systems

1. Wide Area Work Flow (WAWF)

Unless using another means of invoicing, performers will be required to submit invoices for payment directly via to https://wawf.eb.mil. Registration in WAWF will be required prior to any award under this BAA.

2. i-Edison

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

VII. Agency Contacts

Administrative, technical or contractual questions should be sent via e-mail to HR001117S0023@darpa.mil. All requests must include the name, email address, and phone number of a point of contact.

The technical POC for this effort is:

Dr. Linton Salmon
DARPA/MTO
ATTN: HR001117S0023
675 North Randolph Street
Arlington, VA 22203-2114

Email: HR00117S0023@darpa.mil

VIII. Other Information

A. Proposers Day

The SSITH Proposers Day will be held on April 21, 2017 in Arlington, VA. Advance registration is required. See DARPA-SN-17-31 posted at www.fbo.gov for all details. Attendance at the SSITH Proposers Day is not required to propose to this solicitation.

B. Protesting

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