Broad Agency Announcement

Signature Management using Operational Knowledge and Environments (SMOKE)

INFORMATION INNOVATION OFFICE

HR001122S0006

12/6/2021

TABLE OF CONTENTS

PART I: OVERVIEW INFORMATION 3

PART II: FULL TEXT OF ANNOUNCEMENT 4

I. Funding Opportunity Description 4

A. Program Overview 4

B. Program Structure 7

C. Program Phases and Metrics 13

D. Government-Furnished Property/Equipment/Information 17

E. Intellectual Property 17

II. Award Information 17

A. General Award Information 17

B. Fundamental Research 18

III. Eligibility Information 19

A. Eligible Applicants 19

B. Organizational Conflicts of Interest 20

C. Cost Sharing/Matching 21

D. Other Eligibility Criteria 21

IV. Application and Submission Information 22

A. Address to Request Application Package 22

B. Content and Form of Application Submission 22

V. Application Review Information 32

A. Evaluation Criteria 32

B. Review of Proposals 33

VI. Award Administration Information 34

A. Selection Notices and Notifications 34

B. Administrative and National Policy Requirements 34

C. Reporting 35

D. Electronic Systems 35

E. DARPA Embedded Entrepreneur Initiative (EEI) 35

VII. Agency Contacts 37

VIII. Other Information 37

IX. APPENDIX 1 – PROPOSAL SUMMARY SLIDE 39

PART I: OVERVIEW INFORMATION

- **Federal Agency Name** – Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)
- **Funding Opportunity Title** – Signature Management using Operational Knowledge and Environments (SMOKE)
- **Announcement Type** – Initial announcement
- **Funding Opportunity Number** – HR001122S0006
- **Catalog of Federal Domestic Assistance Numbers (CFDA)** – Not applicable.
- **Dates**
  - Posting Date: December 6, 2021
  - Proposers Day: December 7, 2021
  - Questions Due: January 25, 2022, 12:00 noon, Eastern Time
  - Proposal Due Date: January 31, 2022, 12:00 noon, Eastern Time
  - Solicitation Closing Date: May 30, 2022, 5:00 pm, Eastern Time
- **Program Overview** – The SMOKE program will develop signature management technologies that generate evasive cyber infrastructure by incorporating counter-attribution techniques into the design process; quantitatively measuring attribution risk in real-time; and by maintaining evasiveness after infrastructure changes in order to accelerate red team cyber operations (CO) and eliminate signatures as a source of attribution.
- **Anticipated Individual Awards** – There are two technical areas for this solicitation. Multiple awards are anticipated in Technical Area 1 and Technical Area 2.
- **Types of Instruments that May be Awarded** – Procurement Contracts, or Other Transactions for Prototype
- **Agency Contacts**
  - Points of Contact

    The BAA Coordinator for this effort can be reached at:
    Email: SMOKE@darpa.mil
    DARPA/I2O
    ATTN: HR001122S0006
    675 North Randolph Street
    Arlington, VA 22203-2114

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

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

The Defense Advanced Research Projects Agency (DARPA) is soliciting innovative proposals in the following technical areas:

- signature reduction for red team cyber operations;
- automated generation of evasive cyber infrastructure;
- assessing and quantifying attribution risk for red team cyber operations; and
- signature generation for adversary cyber activities.

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. Program Overview

Introduction and Background

Networks are under persistent threat from malicious cyber actors (MCAs). In response, a growing industry of network security professionals are offering realistic, threat informed assessments of network owners' defensive posture. These assessments are performed by a team of ethical hackers (i.e., the red team) in which they assume the role of sophisticated MCAs and perform a controlled security test in collaboration with network defenders (i.e., the blue team). Red team exercises are designed to exceed simple penetration testing and emulate MCA behaviours as realistically as possible. Realistic emulation of sophisticated cyber threats in a measured exercise is very helpful for providing a comprehensive picture of network defenders' readiness.

Towards the aim of realism, red teams plan and deploy tactics, techniques, and procedures (TTPs) that mimic the most advanced cyber threats. Red teams use these TTPs to evade network defenders in order to achieve assessment objectives (e.g., move laterally in networks) and assess how critical networks and mission platforms fare against true MCAs.

A core aspect of red team security assessments are the TTPs used to build and deploy operational infrastructure (e.g., domain names, IP addresses, virtual servers) used for command and control (C2) of red team tools. This infrastructure must exist openly on the public Internet and emits signals that, if detected too easily, can end the assessment quickly without much gain, but at considerable expense. Repeated detection events can lead to patterns which can be crafted into signatures used to attribute red team activities. Signatures are characteristic patterns of the way an operator or organization performs cyber operations. Attribution is the ability to associate a cyber-attack with a responsible party through technical means such as detection and characterization of MCA behaviours (i.e., signatures) observed external to the assessed network. For example, a class of attribution techniques discover patterns in associations to previously attributed cyber infrastructure. Security assessments can end quickly if the blue team prematurely detects these "guilt-by-association" indicators inside of the assessed network. The premature termination of an assessment is unfortunate, but limited to that specific engagement. If the blue team attributes those indicators to additional infrastructure outside of the assessed network, then the red team stands to lose infrastructure used across multiple network assessment engagements having consequences that outlast the current security assessment. This impairs the long-term effectiveness of the red team and thus requires more time and expense to recover.

The preparation of operational infrastructure that emulates sophisticated threats, evades detection, and reduces signatures requires a significant amount of time and subject matter expertise. Today, red teams study historic security incidents for TTPs of MCAs as attributed by cyber threat analysts and manually generate plans that emulate these threat actors. Indeed, red team operators transform informally documented notes into functional infrastructure and make large numbers of complex, interdependent decisions when deploying this infrastructure. Each decision generates observable emissions that form signatures across a variety of cyber datasets. Such a manual approach to operational infrastructure creates attributable signatures and makes increasing the number of concurrent assessments difficult.

Today, the demand for network security assessments is greater than the supply because of a shortage of cyber expertise[1] and a lack of automation. If successful, SMOKE will develop tools to automate the planning and deployment of threat emulated, attribution-aware cyber infrastructure. These tools will enable red teams to increase the scale, efficiency, duration, and effectiveness of cyber security assessments. Moreover, red teams will be able to provide longer cyber security assessments for a larger number of concurrent networks because of their ability to remain hidden for longer.

To improve the effectiveness of security assessments, the DARPA Information Innovation Office (I2O) is soliciting innovative research proposals for the development of tools that enable automated, scalable, and threat-emulated cyber infrastructure. In addition, these tools need to handle the management of the cyber infrastructure lifecycle (i.e., acquisition, usage, and disposal). The SMOKE program will develop, demonstrate, and evaluate these tools through red team security assessments on a range of diverse and realistic networks of interest.

Exemplary SMOKE Use Cases

The following discussion of exemplary use cases is provided to give concrete examples for some of the challenges the solutions may address. Proposers are encouraged to enhance it with other relevant challenges, systems, and solutions as needed to demonstrate technological acumen.

[1] Director, Operational Test & Evaluation FY20 Cybersecurity Cyber Assessments

SMOKE will address the following strategic objectives important to the Department of Defense (DoD):

1. Generation of infrastructure configurations that conform to operational security (OPSEC) risk profiles.

   In the context of red team cyber operation planning, SMOKE will inform cyber planners of attribution risk associated with infrastructure decisions and recommend configurations that adhere to OPSEC risk profiles. To achieve this goal, SMOKE may use a combination of active, passive, and indirect device enumeration and traffic analysis techniques, along with existing relevant data sets (public and/or commercially available), to identify and recommend infrastructure elements for plans that meet or exceed OPSEC requirements. Planning algorithms would need to understand and explain the probabilities of reaching a desired end state using available tools and infrastructure elements as well as the attribution risk associated with each decision. Additionally, to realize these plans, SMOKE may use agents that can safely, reliably, and autonomously acquire, interact, and manage a diverse pool of available infrastructure elements in accordance with mission profiles.

2. Semi-autonomous Persistent Cyber Operations (PCO) for Director, Operational Test & Evaluation (DOT&E) to enable simultaneous cybersecurity assessments for DoD networks.

   To accelerate red team cyber security assessments of DoD networks, SMOKE will automatically generate attack plans and set up C2 infrastructure that emulates advanced cyber threats. To achieve this goal, SMOKE will develop analytics that extract adversary signatures from relevant data sets (public and/or commercially available) and encode those signatures into recommended infrastructure plans. Red teams can choose which plans to execute and task SMOKE autonomous agents to set up and manage C2 infrastructure for simultaneous cybersecurity assessments of multiple DoD networks.

3. Real-time attribution risk assessments/feedback for cyber infrastructure and operational emissions.

   For continuous surveillance of existing cyber infrastructure, SMOKE will provide real-time feedback on infrastructure and operational emissions that may lead to discovery by adversaries or other cyber defenders. To achieve this goal, SMOKE will develop sensors that can monitor infrastructure artifacts that appear in public or commercial datasets and provide real-time attribution risk assessments to ensure infrastructure remains within operational security requirements.

Program Scope

The SMOKE program will develop data-driven tools to automate the planning and execution of threat emulated cyber infrastructure needed for network security assessments (e.g., red team exercises). In a complementary activity, SMOKE will develop data-driven tools to automate the discovery of distinguishable patterns of sophisticated cyber threat infrastructure (i.e., signatures).

Together, SMOKE will prototype components that enable red teams to plan, build, and deploy cyber infrastructure that is informed by machine-readable signatures of sophisticated cyber threats.

Infrastructure planning research that fails to consider realistic network environments is out of scope. Likewise, signature discovery research that fails to provide real-time feedback to infrastructure planning is out of scope.

To ensure realism, SMOKE components will be evaluated on real-world networks controlled by SMOKE performers and/or Government partners. Initially, plans will be executed in simulated or emulated environments created by SMOKE performers. As components mature, plans may be executed on live networks as part of red team network security assessments. Further details on these use cases are described in Section I.A., *Exemplary SMOKE Use Cases*. Successful components may become candidates for transition.

Transition of SMOKE components is a priority and potential transition partners may include organizations such as DOT&E, DoD Services, and other Government organizations. Early and continuous input from SMOKE transition partners will ensure relevance and provide SMOKE with an understanding of the rapidly evolving state of security assessments. Proposers should explain how their approach will support experts in red team network assessments.

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

- Abstracting away complexities of diverse network environments;
- Operating in partially denied environments, reasoning under uncertainty, and reacting to unforeseen detection and/or attribution events;
- Measuring tradeoffs among efficiency and effectiveness of plans in terms of speed and evasion;
- Overcoming state space explosion of typical models for cyber infrastructure planning;
- Developing mechanisms to acquire, manage, and maintain infrastructure elements that conform to signature management policies;
- Executing infrastructure changes in accordance with real-time attribution assessments and plan contingencies;
- Discovering latent associations between infrastructure artifacts;
- Automating expert judgements used to build and traverse infrastructure associations; and
- Expanding our knowledge of adversary infrastructure.

B. Program Structure

SMOKE is a three-year effort divided into two 18-month phases. Phase 1 will focus on developing, demonstrating, and evaluating individual components. Phase 2 will focus on comparative evaluations formed by integrating program components. Not all efforts will align directly with program phases, so proposers should plan to adjust schedules based on results of Government evaluations and transition opportunities.

SMOKE will be divided into two technical areas (TAs) that will work in parallel throughout the program:

- TA1 – Automated Planning and Execution of Attribution-Aware Cyber Infrastructure
- TA2 – Discover and Generate Infrastructure Signatures

It is expected that TA1 and TA2 performers will deliver components on an iterative and incremental basis to transition partners by leveraging the Constellation Pipeline described in this section, where they will be integrated into existing mission platforms for test and evaluation.

Proposers may only submit one proposal as lead institution per TA. Proposals must address only one TA. Proposers may submit as lead institution for **at most** two proposals, one for TA1 and one for TA2. Proposers may be selected for no TA awards, a TA1 award, a TA2 award, or two awards, namely for TA1 and TA2.

Proposers are strongly encouraged to offer up to two (2), 12-month options for additional integration work that will take place within the Constellation Pipeline in parallel and/or beyond the three-year research and development portion of the program. In addition, proposers are encouraged to identify additional technologies that increase the operational use cases and associate them to proposal options. These options and their optional add-ons may or may not be exercised at the sole discretion of the Government.

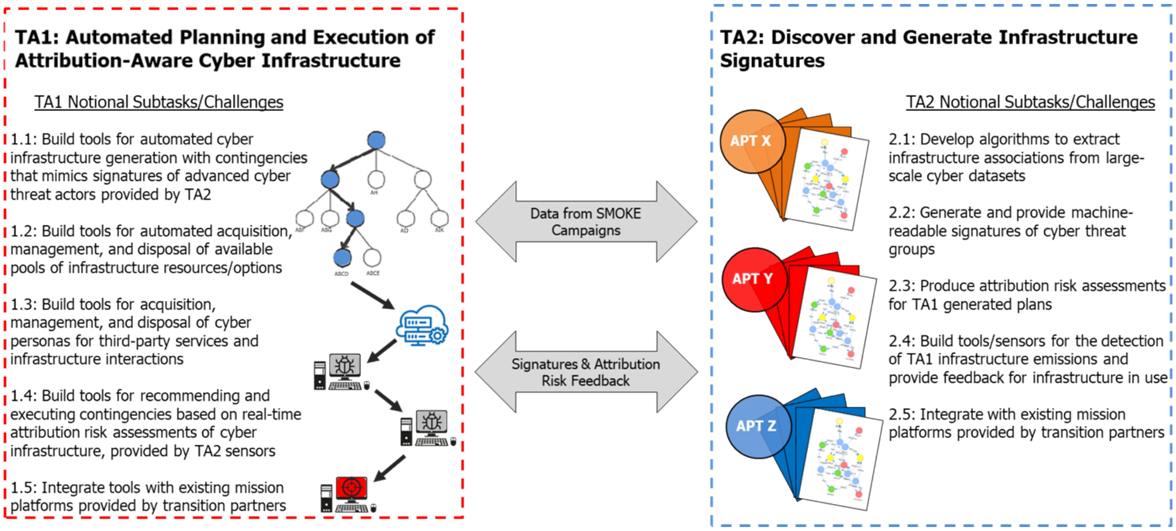
The selected SMOKE performers are required to collaborate with each other. The Government has determined that an Associate Contractor Agreement (ACA) is necessary to help facilitate an open exchange of information and ensure complete compatibility between software components, the system architecture, equipment, data, and other program elements to prevent unnecessary duplication of effort, and to maximize commonality to guarantee appropriate coordination and integration of work. All selected performers will be required to have their ACAs in place prior to the program kick-off meeting.

The Government will assess performer progress with regular technology evaluations and adversarial engagements driven by specific operational scenarios. The operational scenarios may incorporate red teams, U.S. Government cyber operators, and other elements. DARPA encourages technical efforts that allow for flexibility in testing and evaluation to take advantage of opportunities to access data sets under time constraints while permitting long-term research and development.

Proposers addressing either TA1 or TA2 may benefit from having personnel with Top Secret clearances that are eligible for Sensitive Compartmented Information (SCI) and, in particular, a Principal Investigator (PI) that has a Top Secret clearance and is eligible for SCI. Having cleared personnel or a cleared PI is not a requirement and will not be considered during TA1 and TA2 evaluations. **Academic institution and small company participation is explicitly encouraged, regardless of any possession of security clearances.**

Technical Areas

DARPA seeks innovative proposals in the following TAs, as shown in Figure 1 and described in detail as follows:



TA1: Automated Planning and Execution of Attribution-Aware Cyber Infrastructure

TA1 Notional Subtasks/Challenges

1.1: Build tools for automated cyber infrastructure generation with contingencies that mimics signatures of advanced cyber threat actors provided by TA2

1.2: Build tools for automated acquisition, management, and disposal of available pools of infrastructure resources/options

1.3: Build tools for acquisition, management, and disposal of cyber personas for third-party services and infrastructure interactions

1.4: Build tools for recommending and executing contingencies based on real-time attribution risk assessments of cyber infrastructure, provided by TA2 sensors

1.5: Integrate tools with existing mission platforms provided by transition partners

Data from SMOKE Campaigns
Signatures & Attribution Risk Feedback
APT X
APT Y
APT Z

TA2: Discover and Generate Infrastructure Signatures

TA2 Notional Subtasks/Challenges

2.1: Develop algorithms to extract infrastructure associations from large-scale cyber datasets

2.2: Generate and provide machine-readable signatures of cyber threat groups

2.3: Produce attribution risk assessments for TA1 generated plans

2.4: Build tools/sensors for the detection of TA1 infrastructure emissions and provide feedback for infrastructure in use

2.5: Integrate with existing mission platforms provided by transition partners

Figure 1: SMOKE TAs with notional subtasks and challenges

The Government anticipates multiple awards for both technical areas. Proposers are encouraged to read descriptions of both TAs to ensure full understanding of the program context and anticipated feedback loops between performer efforts.

TA1 – Automated Planning and Execution of Attribution Aware Cyber Infrastructure

The goal of TA1 is to plan, build, and deploy threat emulated cyber infrastructure that is required for network security assessments. TA1 has five objectives:

1. Build tools for automated cyber infrastructure generation with contingencies that mimics signatures of advanced cyber threat actors provided by TA2.
2. Build tools for automated acquisition, management, and disposal of available pools of infrastructure resources/options.
3. Build tools for acquisition, management, and disposal of cyber personas for third-party services and infrastructure interactions.
4. Build tools for recommending and executing contingencies based on real-time attribution risk assessments of cyber infrastructure, provided by TA2 sensors.
5. Integrate tools with existing mission platforms provided by transition partners.

TA1 proposals must describe an innovative, data-driven approach to modeling threat emulated cyber infrastructure plans that can be used for security assessments of diverse and complex networks. TA1 approaches must be able to generate infrastructure plans that can evade detection or emulate adversary activity by conforming to TA2-provided signatures. Approaches must also be able to recommend contingency infrastructure plans when the risk of attribution becomes too high.

Additionally, teams will build tools to realize infrastructure plans as components and will evaluate them during simulated operations in real-world network environments (e.g., red team security assessments). Approaches must be deployable and capable of acquiring, interacting, managing, and disposing of infrastructure elements in accordance with desired adversary signatures. TA1 approaches must also be capable of reaching a target network automatically so red team operators can focus on actions within the target network. TA1 solutions will be customized for integration into multiple mission platforms and will permit repeatable and scalable red team security assessments on networks of interest.

Strong proposals will consider using reinforcement learning techniques to reason about plans under uncertainty and incorporate information about attribution into cyber infrastructure decisions or explain why their approach has the potential to produce better results. TA1 components will need to consider tradeoffs between efficiency and effectiveness of plans in terms of speed and evasion. Strong proposals will also consider extending current cyber range and infrastructure as code technologies to realize infrastructure plans via a platform capable of deploying, managing, and continuously monitoring a globally diverse set of infrastructure elements.

The primary challenges for TA1 are the accuracy, scale, diversity, and speed of plan generation and execution. DARPA will facilitate access to relevant data sources by leveraging commercial relationships, U.S. Government (USG) partners, and data exchange agreements. Proposers are strongly encouraged to propose their own data sources and methods, and to identify their data needs concretely. Proposers are strongly encouraged to offer up separate, costed options for program-wide access to their own data sources. These options may or may not be exercised at the Government's sole discretion. Of particular interest are data sources that enable the characterization of real-time global networks for candidate infrastructure elements.

TA1 proposals should, at a minimum, address the following topics:

1. Methods to abstract away complexities of diverse network environments so autonomous agents can learn infrastructure configurations (i.e., plans) that are capable of reaching a target network and maintain C2;
2. Methods to operate in partially denied environments and to reason under uncertainty, gain information about attribution risks, and react to unforeseen detection or attribution events; and
3. Planning algorithms to measure the tradeoff among efficiency and effectiveness in terms of speed and evasion.

Proposers should additionally discuss how their solutions will provide insights as to how infrastructure plans either conform to or evade a set of signatures.

TA2 – Discover and Generate Infrastructure Signatures

The goal of TA2 is to develop technologies to generate adversary cyber signatures that will inform the automated preparation of cyber infrastructures used during network security assessments. TA2 has the following five objectives:

1. Develop algorithms to extract infrastructure associations from large-scale cyber datasets;
2. Generate and provide machine-readable signatures of cyber threat groups;
3. Produce attribution risk assessments for TA1 generated plans;
4. Build tools/sensors for the detection of TA1 infrastructure emissions and provide feedback for infrastructure in use; and
5. Integrate with existing mission platforms provided by transition partners.

TA2 proposals must describe an innovative, data-driven approach to discover cyber infrastructure signatures. Approaches must focus on infrastructure signatures that are useful for attribution and lend themselves to automation. In addition, approaches must generate machine-readable signatures that TA1 approaches can mimic. Approaches must also inform red teams of the attribution risk associated with their infrastructure decisions. TA2 proposals must describe how an approach will learn cyber infrastructure patterns and model infrastructure associations of cyber threat groups hidden in global Internet datasets.

Strong proposals will consider machine-learning approaches to model infrastructure associations through automated pattern recognition and graph-based inferences. Of particular interest are techniques that can extract useful attribution features from global Internet datasets, explain attribution risks to cyber operators for infrastructure in use, and predict if infrastructure configurations can evade or conform to discovered signatures.

The primary challenges for TA2 are the accuracy and effectiveness of adversary signatures and risk assessments. DARPA will facilitate access to relevant data sources by leveraging commercial relationships, USG partners, and data exchange agreements. Proposers are encouraged to propose their own data sources and methods, and to identify their data needs concretely. Proposers are strongly encouraged to offer up separate, costed options for program-wide access to their own data sources. These options may or may not be exercised at the Government's sole discretion. Of particular interest are data sources that enable the extraction of historical and current adversary signatures.

TA2 proposals should at a minimum address the following topics:

1. Generating adversary signatures requires discovering associations between infrastructure elements. Proposers should address how their solutions will extract associations from large-scale cyber datasets and build graph-based models from those associations;
2. To achieve the scale of signatures required for informing TA1 plan generation, TA2 requires unsupervised learning techniques to build and traverse associations. Proposers should discuss how their solutions will build and measure associations with the same quality as subject matter experts and be able to explain attribution assessments to red team operators;
3. Proposals should discuss how their automated approaches can be used by non-experts in attribution and should minimize as much human intervention as possible; and
4. Discovering signatures of cyber infrastructure requires using real-world network traffic datasets. Proposers should discuss how their solutions will generate useful statistics that can be used by planners to predict how well infrastructure configurations will conform or

evade desired signatures and capture SMOKE emissions during red team security assessments to provide feedback.

Requirements for Both TA1 and TA2 Proposals

TA1 and TA2 components will form a feedback loop, as shown in Figures 1 and 2. The feedback loop will enable detection and characterization of TA1 plans. TA1 proposals should explain how their components will generate risk assessment requests. TA2 proposals should explain how their components will incorporate TA1 plans (e.g., ground truth) into their algorithms during research and development (see grey dotted line in Figure 2). Both TA1 and TA2 performers should plan on coordinating closely with each other and proposals should discuss methods for expanding upon proposed feedback mechanisms between TAs.

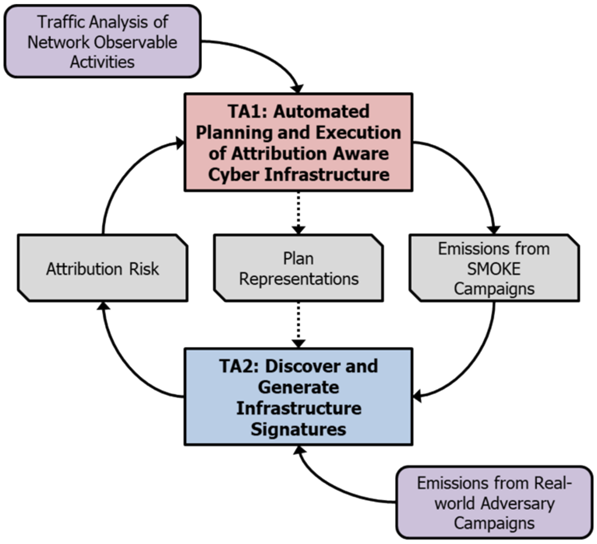

Traffic Analysis of Network Observable Activities
TA1: Automated Planning and Execution of Attribution Aware Cyber Infrastructure
Attribution Risk
Plan Representations
Emissions from SMOKE Campaigns
TA2: Discover and Generate Infrastructure Signatures
Emissions from Real-world Adversary Campaigns

Figure 2: TA1 and TA2 proposals should address how Plan Representations and Attribution Risk Feedback will be exchanged

Information Only Transition Support Activity (i.e., Constellation Pipeline)

The following section is provided as information only to aid proposers in preparing their proposal submissions.

DARPA will establish a user-directed, incremental, and iterative DevSecOps (development, security, and operations) pipeline to accelerate the creation, adoption, and delivery of SMOKE components into U.S. Cyber Command, DOT&E, and other transition partner software ecosystems. The Constellation Pipeline will provide an environment where operational users, developers, and researchers can engage collaboratively in the creative process to converge on solutions that neither group would conceive in isolation. To this end, in-person tech exchanges, hackathons, and virtual technical exchanges will be planned once development environments become operational. As capabilities mature, pilot tests with operational user communities of significant size and diversity will be conducted to assess the viability and generality of the approaches. Ultimately, pilot tests will span across services, user communities, and combatant commands (COCOMs) to ensure that capabilities provide value to diverse stakeholders.

Proposals should discuss how their components could leverage the Constellation Pipeline and integrate with relevant Government mission platforms. Proposals should also discuss existing relationships with Government partners, Government development networks, and Government mission platforms.

C. Program Phases and Metrics

The SMOKE program is a 36-month effort divided into two 18-month phases. Phase 1 will focus on developing, demonstrating, and evaluating individual components. Phase 2 will focus on comparative evaluations formed by integrating program components.

SMOKE will evaluate components on networks of interest as part of real-world security assessments performed by red team partners. Each exercise will be designed by an Independent Verification and Validation (IV&V) team that will generate multiple scenarios informed by prior related I2O efforts to simulate operations. SMOKE TA1 metrics focus on time, scalability, and attribution. TA1 components will be evaluated on the ability of cyber operators to reduce cyber operations' response time – and the ability to launch and maintain multiple concurrent operations without being attributed. In addition, infrastructure plans will be judged by their ability to confound attribution, reconstitute infrastructure after attribution, and explain the rationale behind automated decisions to red team partners. SMOKE TA2 metrics focus on generating and detecting signatures. TA2 components will be measured according to how well signatures match the judgement of attribution experts, how well attribution risk assessment matches emulations, and how well they can be incorporated as sensors that provide meaningful feedback.

Precision and recall will be used to measure detection and attribution performance. Precision, recall, and F_1 are three metrics that are commonly used to measure detection performance. To this end, we define a true positive as a detection of an infrastructure element (e.g., host, user, or network address) that was used in a TA1 plan (e.g., emulated threat), and a false positive is defined as an identified infrastructure element that was not used in a TA1 plan. Similarly, a false negative is defined as an infrastructure element that was missed and a true negative is an infrastructure element that was not used in a TA1 plan. Likewise, precision, recall, and F_1 are three metrics that are commonly used to measure attribution performance. To this end, we define a true positive as a correct attribution of infrastructure elements used in a TA1 plan (i.e., actual TA1 threat actor), and a false positive is defined as misattributed infrastructure elements that was used in a TA1 plan (i.e., emulated threat actor). Similarly, false negative is defined as the inability to attribute infrastructure elements and a true negative as identification of benign infrastructure elements.

During the first phase, SMOKE will define the initial operationally-relevant baselines for precision and recall (See Table 1); as well as measure speed and scalability of deployment. Phase 2 will improve upon the initial baselines and will define additional metrics for evaluating performance.

TAs	Metrics	Phase 1 Objectives	Phase 2 Objectives
TA1 (Planning and Execution)	Precision and recall for blue team attribution	Establish blue team baseline and reduce it by 10%	Establish blue team baseline and reduce it by 25%

	Number of nodes in simulated network	At least 3 networks with 100 nodes	At least 30 networks with 1000 nodes
	Time to develop plan	Within 8 hours	Within 60 minutes
	Number of concurrent attack plan emulations	2	20
	Emulate multiple environments in parallel	10	100
	Time to deploy infrastructure	Within 2 days	Within 8 hours
	Integrated demonstration with TA2	In emulated environments	In real-world environments (e.g., red team security assessments)
TA2 (Signatures)	# of Advanced Persistent Threats	2	5
	Precision and recall for blue team attribution	Establish blue team baseline and increase it by 10%	Establish blue team baseline and increase it by 25%

Table 1: SMOKE Metrics

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

Schedule and Milestones

For each year of effort, there will be quarterly meetings with the Program Manager (PM), consisting of two (2) alternating technical exchanges and two (2) alternating integrated demonstrations. During these meetings/reviews, the PM will assess progress towards the solution via performer briefings, technical discussions, integrated demonstrations, and evaluation/challenge exercises. At the end of each phase, SMOKE will conduct pilot tests with operational users to integrate SMOKE components into existing workflows and mission platforms. Once the Constellation Pipeline is operational, the goal will be to host integrated demonstrations and pilot tests within the Constellation's development environment.

These quarterly meetings will focus on open technical exchange and demonstration of SMOKE capabilities on realistic challenge problems, in real-world environments, and in collaboration with operational users. Difficulties encountered and possible solutions will also be discussed. The goals of the quarterly technical exchanges and integrated demonstrations will be to: (1) review and share innovations/accomplishments of the SMOKE program; (2) review and discuss plans and options for technology demonstrations and prototypes; (3) review and discuss results from meetings and events conducted prior to and after the tests and evaluation/challenge exercises; (4) demonstrate prototypes; and (5) plan for the next six-month period.

The Government will specify the locations for the technical interchanges and PI meetings. For budgeting purposes, assume the locations of the two PI meetings held each year will alternate between Washington, D.C. and San Diego, CA. In addition to site visits, regular teleconference meetings are encouraged to enhance communications and collaborations, as required, among the performers. Should important issues arise between program reviews, the Government team will be available to support informal meetings. In-person meetings, evaluations, and site visits may be replaced with virtual ones, if necessary.

Figure 3 below provides a tentative program schedule. Proposers should propose a detailed schedule that is consistent with the maturity of their approaches and the risk reduction required for their concepts and their program plan. These schedules will be synchronized across performers, as required, and monitored and revised as necessary throughout the SMOKE program's period of performance. A start timeframe of August 2022, should be assumed for budgeting purposes.

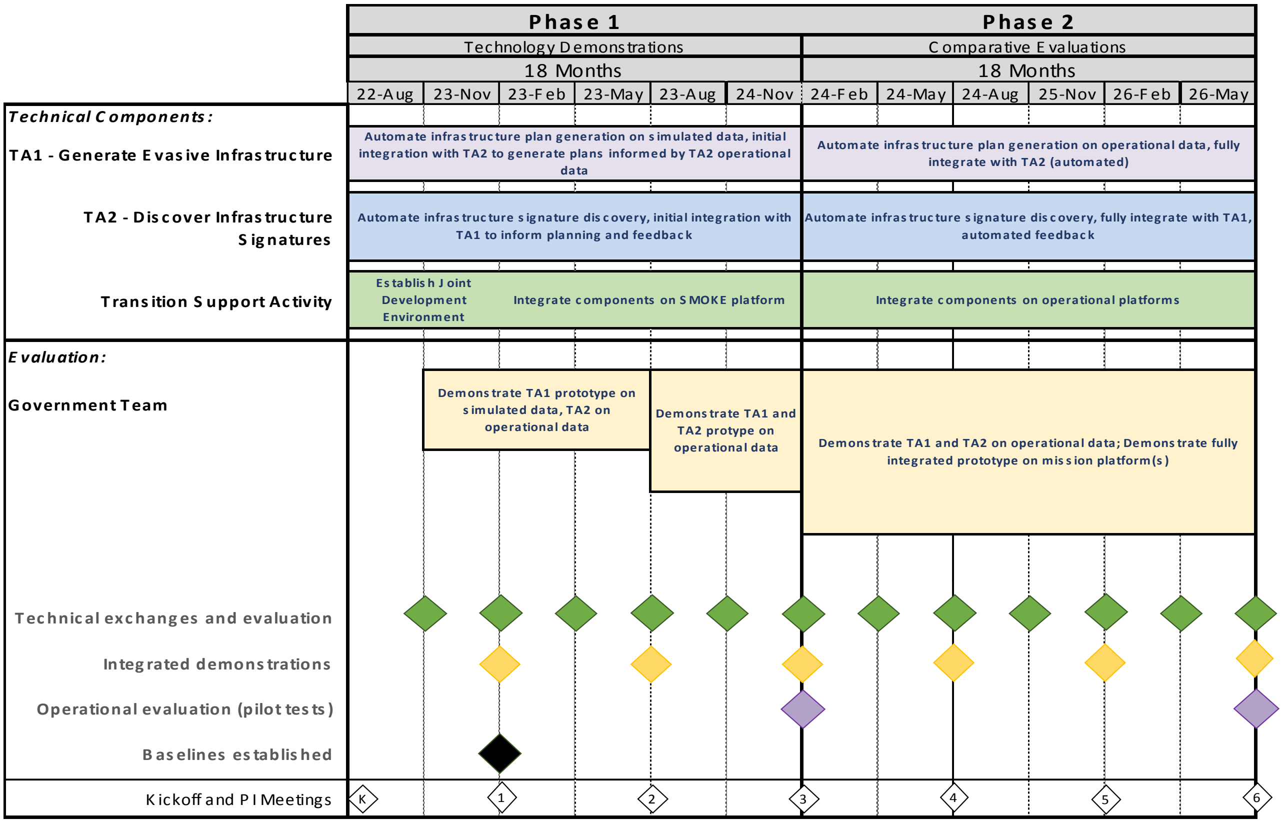


Figure 3: SMOKE Tentative Program Schedule

Deliverables

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

- Slide Presentations – Annotated slide presentations will be submitted within two weeks after program kick-off meeting and after each review.
- Quarterly Technical Status Reports – A quarterly technical status report to the DARPA Vault reporting system describing progress made, resources expended, and any issues requiring the attention of the Government team will be provided within 10 calendar days after the end of each quarter.
- Monthly Financial Reporting – Monthly expenditure reports and uploading of required deliverables to the DARPA Vault reporting system are required by all SMOKE performers.
- System Development Plan (SDP) –The SDPs for each phase will be based on the performers' proposal and will be presented at the kickoff meeting for each phase. The SDP will describe the scope of the design and development effort, describe the hardware and software architecture in sufficient detail for review and planning, reference any applicable documents, and provide a program schedule. A SDP deliverable will be submitted within one month after the kickoff meeting for each phase, and shared with other performers for synchronization.
- Software – All computer software delivered under the SMOKE program must be delivered as source and object executable code. Include the source listings and source code for the target computer systems, as well as any build scripts or other technical information required for the Government to compile all delivered source code. Delivered software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation.
- Software Documentation – Software documentation deliverables will be provided within one month after the end of each phase documenting source code, hardware description language specifications, system diagrams, part numbers, and other data necessary to maintain and to produce copies of the software.
- Hardware – At the conclusion of the period of performance, all hardware procured or developed under the SMOKE program will be delivered to the Government. The delivered components will be the same as those used to perform final performance tests and evaluations at the end of the period of performance. The delivery should include sufficient documentation to be completely operable, maintainable, and modifiable, with no reliance on any non-delivered hardware or hardware documentation developed or procured under the SMOKE program.
- Phase and Final Technical Reporting – End-of-phase reports are due at the conclusion of each phase, including through final phase contract completion. A separate Final Technical Report is due at the end of the period of performance. The reports will concisely summarize the effort conducted and provide any lessons learned during the development of the SMOKE technology, and should be delivered to the DARPA Vault reporting system.

- Science & Technology Program Implementation Plan (S&T PIP) – One plan covering TA1 and TA2, as applicable. Due 30 calendar days prior to executing sensitive testing and updates as required by DARPA Program Security.

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

D. Government-Furnished Property/Equipment/Information

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

E. Intellectual Property

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

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

II. Award Information

A. General Award Information

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

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

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

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

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

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

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

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

For certain research projects, it may be possible that although the research to be performed by a potential awardee is non-fundamental research, its proposed subawardee's effort may be fundamental research. It is also possible that the research performed by a potential awardee is fundamental research while its proposed subawardee's effort may be non-fundamental research. In all cases, it is the potential awardee's responsibility to explain in its proposal which proposed efforts are fundamental research and why the proposed efforts should be considered fundamental research.

III. Eligibility Information

A. Eligible Applicants

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

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

a) FFRDCs

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

b) Government Entities

Government Entities (e.g., Government/National laboratories, military educational institutions, etc.) are subject to applicable direct competition limitations. Government Entities must clearly demonstrate that the work is not otherwise available from the private sector and provide written documentation citing the specific statutory authority and contractual authority, if relevant, establishing their ability to propose to Government solicitations and compete with industry. This information is required for Government Entities proposing to be awardees or subawardees.

c) Authority and Eligibility

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

2. Other Applicants

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

B. Organizational Conflicts of Interest

FAR 9.5 Requirements

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

Agency Supplemental OCI Policy

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

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

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

Government Procedures

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

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

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

C. Cost Sharing/Matching

Cost sharing is not required; however, it will be carefully considered where there is an applicable statutory condition relating to the selected funding instrument. Cost sharing is encouraged where there is a reasonable probability of a potential commercial application related to the proposed research and development effort.

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

D. Other Eligibility Criteria

Ability to Support Classified Development

Proposers addressing either TA1 or TA2 may benefit from having personnel with Top Secret clearances that are eligible for SCI and, in particular, a PI that has a Top Secret clearance and is eligible for SCI. Having cleared personnel or a cleared PI is not a requirement and will not be considered during TA1 and TA2 evaluations. **Academic institution and small company participation is explicitly encouraged, regardless of any possession of security clearances.**

IV. Application and Submission Information

A. Address to Request Application Package

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

B. Content and Form of Application Submission

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

1. Proposals Format

All proposals should be in the format given below. The typical proposal should express a consolidated effort in support of one or more related technical concepts or ideas. Disjointed efforts should not be included into a single proposal. Proposals shall consist of two volumes: 1) Volume I, Technical and Management Proposal (composed of three [3] Sections); and 2) Volume II, Cost Proposal. The maximum page count for Volume I, Technical and Management Proposal, is 30 pages including all figures, tables, and charts, but not including the cover sheet, summary slide, and any table of contents, or appendices. A submission letter is optional and is also not included in the page count.

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

a) Volume I, Technical and Management Proposal

(1) Section I: Administrative

(a) Cover Sheet to Include

(1) BAA number (HR001122S0006);
(2) Technical area;
(3) Lead Organization submitting proposal;
(4) Type of organization, selected among the following categories: “LARGE BUSINESS”, “SMALL DISADVANTAGED BUSINESS”, “OTHER SMALL BUSINESS”, “HBCU”, “MI”, “OTHER EDUCATIONAL”, OR “OTHER NONPROFIT”;
(5) Proposer’s reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;
(8) Technical point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, electronic mail (if available);

(9) Administrative point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, electronic mail (if available);
(10) Total funds requested from DARPA, and the amount of cost share (if any); AND
(11) Date proposal was submitted.

(b) Official transmittal letter

(2) Section II: Summary of Proposal

A. Technical rationale, technical approach, and constructive plan for accomplishment of technical goals in support of innovative claims and deliverable creation.
B. Innovative claims for the proposed research. This section is the centerpiece of the proposal and should succinctly describe the uniqueness and benefits of the proposed approach relative to the current state-of-art alternate approaches.
C. Deliverables associated with the proposed research and the plans and capability to accomplish technology transition and commercialization. Include in this section all proprietary claims to the results, prototypes, intellectual property, or systems supporting and/or necessary for the use of the research, results, and/or prototype. If there are no proprietary claims, this should be stated. For forms to be completed regarding intellectual property, see Section IV.B.2.i of this BAA. There will be no page limit for the listed forms.
D. General discussion of other research in this area.
E. A clearly defined organization chart for the program team which includes, as applicable: (1) the programmatic relationship of team member; (2) the unique capabilities of team members; (3) the task of responsibilities of team members; (4) the teaming strategy among the team members; and (5) the key personnel along with the amount of effort to be expended by each person during each year.
F. A summary slide of the proposed effort, in PowerPoint format, should be submitted with the proposal. Submit this PowerPoint file in addition to Volumes 1 and 2. The format for the summary slide is included as Appendix 1 to this BAA and does not count against the page limit.

(3) Section III: Detailed Proposal Information

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

- Clearly identify any tasks/subtasks (to be performed by either an awardee or subawardee) that will be accomplished on-campus at a university, if applicable.

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

Do not include any proprietary information in the SOW.

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

b) Volume II, Cost Proposal

All proposers, including FFRDCs, must submit the following:

(1) Cover sheet to include:

(1) BAA number (HR001122S0006);
(2) Technical area;
(3) Lead Organization submitting proposal;
(4) Type of organization selected among the following categories: "LARGE BUSINESS", "SMALL DISADVANTAGED BUSINESS", "OTHER SMALL BUSINESS", "HBCU", "MI", "OTHER EDUCATIONAL", OR "OTHER NONPROFIT";
(5) Proposer's reference number (if any);
(6) Other team members (if applicable) and type of organization for each;
(7) Proposal title;

(8) Technical point of contact to include: salutation, last name, first name, street address, city, state, zip code, telephone, 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, 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 for Prototype;
(11) Place(s) and period(s) of performance;
(12) Total proposed cost separated by basic award and option(s) (if any);
(13) Name, address, and telephone number of the proposer's cognizant Defense Contract Management Agency (DCMA) or Office of Naval Research (ONR) administration office (if known);
(14) Name, address, and telephone number of the proposer's cognizant Defense Contract Audit Agency (DCAA) or comparable Educational Institutional audit office (if known);
(15) Date proposal was prepared;
(16) Data Universal Numbering System (DUNS) number;
(17) Taxpayer Identification Number (TIN) number;
(18) Commercial and Government Entity (CAGE) Code;
(19) Subawardee Information; and
(20) Proposal validity period.

(2) Additional Cost Proposal Information

(a) Supporting Cost and Pricing Data

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

(b) Cost Breakdown Information and Format

Detailed cost breakdown to include:

- Total program costs broken down by major cost items (direct labor, including labor categories; subcontracts; materials; other direct costs; overhead charges, etc.) and further broken down by task and phase
- Major program tasks by fiscal year
- An itemization of major subcontracts and equipment purchases.
- Documentation supporting the reasonableness of the proposed equipment costs (vendor quotes, past purchase orders/purchase history, detailed engineering estimates, etc.) shall be provided.
- An itemization of any information technology (IT) purchase, as defined by FAR 2.101 – Documentation supporting the reasonableness of the proposed equipment costs(vendor quotes, past purchase orders/purchase history, detailed engineering

estimates, etc.) shall be provided, including a letter stating why the proposer cannot provide the requested resources from its own funding for prime and all sub-awardees.

- A summary of projected funding requirements by month
- The source, nature, and amount of any industry cost-sharing
- Identification of pricing assumptions of which may require incorporation into the resulting award instrument (e.g., use of Government Furnished Property/Facilities/Information, access to Government Subject Matter experts, etc.)

Tables included in the cost proposal must be in an editable (e.g. MS Excel) format with calculation formulas intact.

The Government strongly encourages that proposers use the provided MS Excel^{TM} DARPA Standard Cost Proposal Spreadsheet in the development of their cost proposals. A customized cost proposal spreadsheet may be an attachment to this solicitation. If not, the spreadsheet can be found on the DARPA website at http://www.darpa.mil/work-with-us/contract-management (under "Resources" on the right-hand side of the webpage). All tabs and tables in the cost proposal spreadsheet should be developed in an editable format with calculation formulas intact to allow traceability of the cost proposal. This cost proposal spreadsheet should be used by the prime organization and all subcontractors. In addition to using the cost proposal spreadsheet, the cost proposal still must include all other items required in this announcement that are not covered by the editable spreadsheet. Subcontractor cost proposal spreadsheets may be submitted directly to the Government by the proposed subcontractor via e-mail to the address in Part I of this solicitation. **Using the provided cost proposal spreadsheet will assist the Government in a rapid analysis of your proposed costs and, if your proposal is selected for a potential award, speed up the negotiation and award execution process**.

NOTE: The cost proposal spreadsheet is a supplement to, and not a substitution for, the Cost Volume. The Cost Volume should be submitted as previously outlined.

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

(c) Subaward Proposals

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

All proprietary subaward proposal documentation, prepared at the same level of detail as that required of the proposer's proposal and which cannot be uploaded with the proposal, shall be provided to the Government either by the proposer or by the subawardee organization when the proposal is submitted. Subawardee proposals submitted to the Government by the proposer's awardee should be submitted electronically to SMOKE@darpa.mil, and the proposed awardee will not be allowed to view. The subawardee must provide the same number of copies to the PCO as is required of the awardee. See Section IV.B.3.a. of this BAA for proposal submission information.

(d) Other Transaction Requests

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

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

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

2. Additional Proposal Information

a) Proprietary Markings

Proposers are responsible for clearly identifying proprietary information. Submissions containing proprietary information must have the cover page and each page containing such information clearly marked with a label such as "Proprietary". NOTE: "Confidential" is a classification marking used to control the dissemination of U.S. Government National Security Information as dictated in Executive Order 13526 and should not be used to identify proprietary business information.

b) Security Information

(1) Program Security Information

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

(2) Controlled Unclassified Information (CUI)

For unclassified proposals containing controlled unclassified information (CUI), applicants will ensure personnel and information systems processing CUI security requirements are in place.

(a) CUI Proposal Markings

If an unclassified submission contains CUI or the suspicion of such, as defined by Executive Order 13556 and 32 CFR Part 2002, the information must be appropriately and conspicuously marked CUI in accordance with DoDI 5200.48. Identification of what is CUI about this DARPA program will be detailed in a DARPA CUI Guide and will be provided as an attachment to the BAA or may be provided at a later date.

(b) CUI Submission Requirements

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

(c) Proposers submitting proposals involving the pursuit and protection of DARPA information designated as CUI must have, or be able to acquire prior to contract award, an information system authorized to process CUI information IAW NIST SP 800-171 and DoDI 8582.01.

(d) Unclassified Submissions

DARPA anticipates that submissions received under this BAA will be unclassified. However, should a proposer wish to submit classified information, an unclassified email must be sent to the BAA mailbox requesting submission instructions from the Technical Office PSO. 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.

(e) Both Classified and Unclassified Submissions

For a proposal that includes both classified and unclassified information, the proposal may be separated into an unclassified portion and a classified portion. The proposal should include as much information as possible in the unclassified portion and use the classified portion ONLY for classified information. The unclassified portion must be submitted through the DARPA BAA Website, per the instructions in Section IV.B.3.a, below. The classified portion must be provided separately, and must follow the "Unclassified Submission" instructions outlined above.

c)

Disclosure of Information and Compliance with Safeguarding Covered Defense Information Controls

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

DFARS 252.204-7000, “Disclosure of Information”
DFARS 252.204-7008, “Compliance with Safeguarding Covered Defense Information Controls”
DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”

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

Compliance with the above requirements includes the mandate for proposers to implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) and DoDI 8582.01 that are in effect at the time the solicitation is issued.

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

d) Representations and Certifications

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

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

e)

Human Subjects Research (HSR)/Animal Use

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

f) Approved Cost Accounting System Documentation

Proposers that do not have a Cost Accounting Standards (CAS) complaint accounting system considered adequate for determining accurate costs that are negotiating a cost- type procurement contract must complete an SF 1408. For more information on CAS compliance, see http://www.dcaa.mil. To facilitate this process, proposers should complete the SF 1408 found at http://www.gsa.gov/portal/forms/download/115778 and submit the completed form with the proposal.

g) Small Business Subcontracting Plan

Pursuant to Section 8(d) of the Small Business Act (15 U.S.C. § 637(d)) and FAR 19.702(a)(1), each proposer who submits a 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.

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

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

i) Intellectual Property

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

(1) For Procurement Contracts

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

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

(2) For All Non-Procurement Contracts

Proposers responding to this BAA requesting 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 (1). above. If no restrictions are intended, then the proposer should state "NONE."

j)

System for Award Management (SAM) and Universal Identifier Requirements

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

International entities can register in SAM by following the instructions in this link: https://www.fsd.gov/sys_attachment.do?sys_id=c08b64ab1b4434109ac5ddb6bc4bcbb8.

3. Submission Information For Proposers Requesting Procurement Contracts or OTs and Submitting to a DARPA-approved Proposal Submissions Website

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 HR001122S0006. Submissions may not be submitted by fax or e-mail; any submission received through fax or e-mail will be disregarded.

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

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

The proposal must be received via DARPA's BAA Website (https://baa.darpa.mil) on or before January 31, 2022, 12:00 noon, Eastern Time, in order to be considered during the initial round of selections; however, proposals received after this deadline may be received and evaluated up to the solicitation closing deadline of May 30, 2022, 5:00 p.m., Eastern Time. Proposals submitted after the due date specified in the BAA, but before the solicitation closing date, may be selected. Proposers are warned that the likelihood of available funding is greatly reduced for proposals submitted after the initial closing date deadline.

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

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

Classified submissions 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. Any classified components should follow the instructions provided in Section IV.B.2.b.

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

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

4. Frequently Asked Questions

DARPA will post a consolidated Frequently Asked Questions (FAQ) document. To access the posting go to: http://www.darpa.mil/work-with-us/opportunities. Under the HR001122S0006 summary will be a link to the FAQ. Submit your question/s by E-mail to SMOKE@darpa.mil. Questions must be received by the FAQ/Questions due date listed in Part I, Overview Information.

V. Application Review Information

A. Evaluation Criteria

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

1. Overall Scientific and Technical Merit

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

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

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

2. Potential Contribution and Relevance to the DARPA Mission

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

3. Cost and Schedule Realism

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

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

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

B. Review of Proposals

1. Review Process

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

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

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

2. Handling of Source Selection Information

DARPA policy is to treat all submissions as source selection information (see FAR 2.101 and 3.104), and to disclose their contents only for the purpose of evaluation. Restrictive notices notwithstanding, during the evaluation process, submissions may be handled by support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors performing this role are expressly prohibited from performing DARPA-sponsored technical research and are bound by appropriate nondisclosure agreements. Subject to the restrictions set forth in FAR 37.203(d), input on technical aspects of the proposals may be solicited by DARPA from non-Government consultants/experts who are strictly bound by the appropriate non-disclosure requirements.

3. Federal Awardee Performance and Integrity Information (FAPIIS)

Per 41 U.S.C. 2313, as implemented by FAR 9.103 and 2 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 and Notifications

Proposals

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

B. Administrative and National Policy Requirements

1. Meeting and Travel Requirements

There will be a program kickoff meeting and all key participants are required to attend. Performers should also anticipate regular program-wide meetings and periodic site visits at the Program Manager’s discretion.

2. Solicitation Provisions and Award Clauses, Terms and Conditions

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

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

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

C. Reporting

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

D. Electronic Systems

1. Wide Area Work Flow (WAWF)

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

2. i-Edison

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

E. DARPA Embedded Entrepreneur Initiative (EEI)

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

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

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

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

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

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

VII. Agency Contacts

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

Points of Contact
The BAA Coordinator and Technical POC for this effort may be reached at SMOKE@darpa.mil.
DARPA/I2O
ATTN: HR001122S0006
675 North Randolph Street
Arlington, VA 22203-2114

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

VIII. Other Information

Proposers Day

A virtual Proposers Day for this effort will be held on December 7, 2021.
The Special Notice regarding this Proposers Day can be found at:
https://www.schafertmd.com/darpa/i2o/SMOKE/pd/

For further information regarding the SMOKE Proposers Day, including slides from the event, please see http://www.darpa.mil/work-with-us/opportunities under HR001122S0006.

Associate Contractor Agreement (ACA)

This same or similar language will be included in procurement contract awards against HR001122S0006. Awards other than FAR based contracts will contain similar agreement language:

(a) It is recognized that success of the SMOKE research effort depends in part upon the open exchange of information between the various Associate Contractors involved in the effort. This language is intended to ensure that there will be appropriate coordination and integration of work by the Associate Contractors to achieve complete compatibility and to prevent unnecessary duplication of effort. By executing this contract, the Contractor assumes the responsibilities of an Associate Contractor. For the purpose of this ACA, the term Contractor includes subsidiaries, affiliates, and organizations under the control of the contractor (e.g., subcontractors).

(b) Work under this contract may involve access to proprietary or confidential data from an Associate Contractor. To the extent that such data is received by the Contractor from any Associate Contractor for the performance of this contract, the Contractor hereby agrees that any proprietary information received shall remain the property of the Associate Contractor and shall be used solely for the purpose of the SMOKE 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.

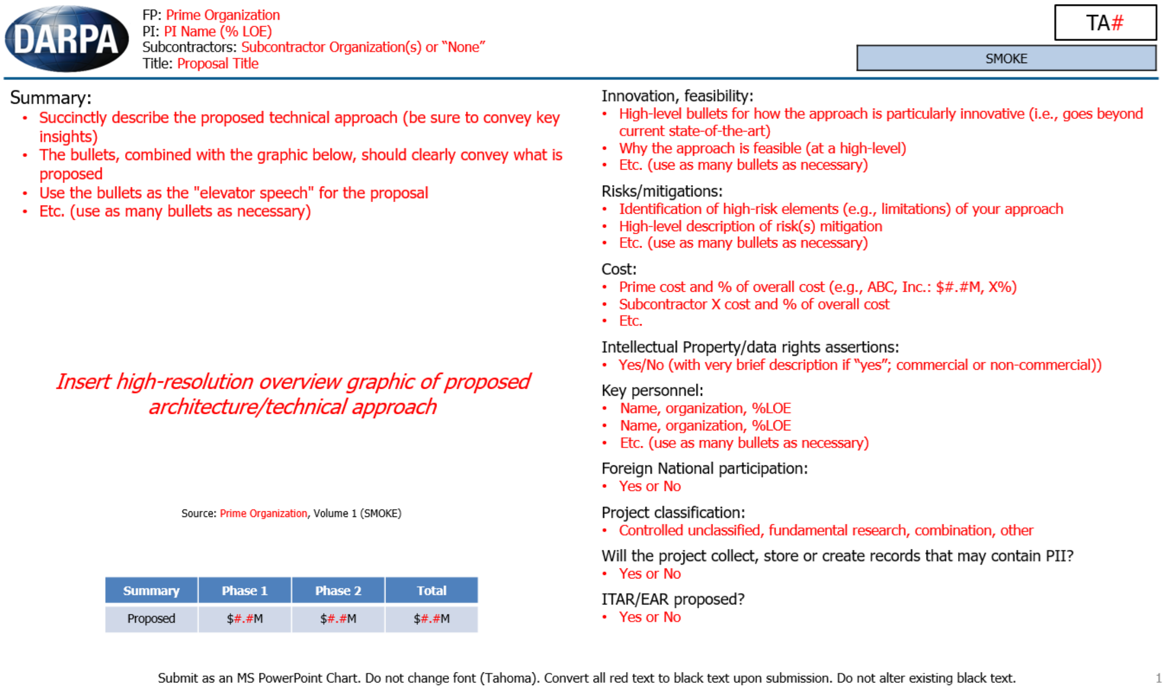
(d) In the event that the Contractor and the Associate Contractor are unable to agree upon any such interface matter of substance, or if the technical data identified is not provided as scheduled, the Contractor shall promptly notify the DARPA SMOKE Program Manager. The Government will determine the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

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

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

Contractor	Technical

IX. APPENDIX 1 – PROPOSAL SUMMARY SLIDE



FP: Prime Organization
PI: PI Name (% LOE)
Subcontractors: Subcontractor Organization(s) or "None"
Title: Proposal Title

TA#

SMOKE

Summary:

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

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

Source: Prime Organization, Volume 1 (SMOKE)

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

Innovation, feasibility:

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

Risks/mitigations:

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

Cost:

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

Intellectual Property/data rights assertions:

- Yes/No (with very brief description if "yes"; commercial or non-commercial))

Key personnel:

- Name, organization, %LOE
- Name, organization, %LOE
- Etc. (use as many bullets as necessary)

Foreign National participation:

- Yes or No

Project classification:

- Controlled unclassified, fundamental research, combination, other

Will the project collect, store or create records that may contain PII?

- Yes or No

ITAR/EAR proposed?

- Yes or No

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

1