Broad Agency Announcement

Information Innovation Office
Securing Artificial Intelligence for Battlefield Effective Robustness (SABER)

HR001125S0009

Amendment 01

April 4, 2025

This publication constitutes a Broad Agency Announcement (BAA) as contemplated in Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016 and 2 CFR § 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.

AMENDMENT 01

The purpose of this Amendment 01 is listed below:

1. Deadline Extensions
    a. Notification of Intent to Prepare Classified Proposal Due Date
    b. Proposal Due Date
    c. Issuance of DD-254s Date

2. Attachment P2: Proposal Instructions and Volume I Template (Technical and Management). The following changes have been made to the template:
    a. The Statement of Work (SOW) and Schedule have been removed from Page limit requirements
    b. The Table of Contents has been updated
    c. A SOW template with instructions has been added to the template
    d. A revision in the Schedule requirements has been updated
    e. Appendix A numbers have been removed from each subject heading

No additional changes have been made to the solicitation.

SECTION I: OVERVIEW

- **Federal Agency Name** – Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)
- **Funding Opportunity Title** – Securing Artificial Intelligence for Battlefield Effective Robustness (SABER)
- **Announcement Type –** Initial Announcement
- **Funding Opportunity Number –** HR001125S0009
- **Assistance Listing Number:** Not Applicable
- **Dates/Time - All Times are Eastern Time Zone (ET)**
  - Posting Date: March 12, 2025
  - Proposers Day: March 12, 2025
  - Proposal Abstract Due Date: March 31, 2025 at 5:00 PM
  - Request for Security Classification Guide: March 31, 2025 at 5:00 PM
  - Notification of Intent to Prepare Classified Proposal: April 24, 2025 at 5:00 PM
  - Question Submittal Closed: March 31, 2025 at 5:00 PM
  - Proposal Due Date: May 20, 2025 at 5:00 PM
- **Anticipated individual awards** - Multiple awards are anticipated.
- **Types of instruments that may be awarded** – Procurement contract or Other Transaction.
- **NAICS Code**: 541715
- **Agency contact**
  - Points of Contact

    The BAA Coordinator for this effort may be reached at:
    SABER@darpa.mil

    DARPA/ I2O
    ATTN: HR001125S0009
    675 North Randolph Street
    Arlington, VA 22203-2114

SECTION II: DEFINITIONS

Table 1 provides the definitions for terms used throughout this Broad Agency Announcement (BAA).

Table 1: SABER Program definitions

Term	Definition
Sensor	A device that detects or measures a physical property and records, indicates, or otherwise responds to it.
Artificial Intelligence (AI)	An algorithm or series of algorithms that interpret data in order to inform a decision. For the purposes of SABER, we will focus on discriminative AI models used to interpret data for inference purposes - as these algorithms will see widespread use in near-term military systems.
AI-enabled Battlefield System	A military system used in battlefield settings containing at least one critical component dependent on the functioning of AI that may be deployed in an adversarial, contested environment.
Cyber	The digital domain or environment where information is exchanged and manipulated through computer networks, essentially representing the interconnected network of computers and systems where cyberspace operations are conducted.
Electronic Warfare (EW)	Use of directed energy emitted over various parts of the electromagnetic spectrum to control the electromagnetic environment and/or degrade sensing instruments sensitive to emissions in the electromagnetic spectrum.
AI Attack Effect	An impact by an adversary's attack on an AI-enabled system that enables them to manipulate its output, degrading or denying the system operation.
AI Attack Vector	A method by which an AI attack effect is caused. Some examples include physical means of manipulating the environments to induce AI errors, cyber means to directly manipulate model-weights in the AI, or EW means of manipulating sensors that feed into a downstream AI pipeline.
AI Kill Chain	A sequence of steps (and maneuvers) utilizing one or more AI attack vectors to enact an AI attack effect against a system.
AI Red Team	An AI red team is a team of experts used to assess the vulnerabilities of the AI-related components of a system pipeline to improve overall security. These teams emulate a potential adversary in AI-enabled system evaluations, attempting a variety of methods for system vulnerability discovery and exploitation.
Operational Test and Evaluation (OT&E)	The testing and evaluation of a system in an operational environment that closely matches the environment and dynamics that a system will face when deployed in a contested operational capacity. The adversary is modeled by a red team.
AI System Under Test (ASUT)	An AI-enabled system evaluated in an OT&E event.
Tactics, Techniques, and Procedures (TTP)	A set of approaches that an adversary (or in the context of OT&E, a red team) may use to systematically gain access and deliver an effect against a system.

SECTION III: FUNDING OPPORTUNITY DESCRIPTION

The Defense Advanced Research Projects Agency (DARPA) is soliciting innovative abstracts and proposals in the following technical domains: the survey, evaluation, selection, development, and integration of techniques and technologies for the creation and employment of red teaming tools that enable the effective operational assessment of AI-enabled battlefield systems, including both ground and air autonomy. Proposed research should investigate innovative approaches that enable revolutionary advances in science, materials, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

Program Goal

Securing Artificial Intelligence for Battlefield Effective Robustness (SABER) will develop an operational AI red teaming construct and framework for OT&E of AI-enabled battlefield systems. This team will assess the operational impacts of vulnerabilities unique to the use of AI, with a focus on the evaluation of near-term AI-enabled autonomous ground and air (rotary wing) capabilities. To that end, research performed under SABER will focus on the development and operationalization of technologies in Physical manufacturing/printing, Adversarial AI, Cyber, EW (PACE), or other technologies into an operational AI red teaming assessment framework and toolkit. The framework and toolkit should enable an AI red team to reliably and rapidly deliver AI attack effects via AI kill chain TTPs to AI-enabled battlefield systems in operational environments.

Program Background

Significant advances in AI are unignorable, and AI is impacting almost every field it is applied to, whether it be image analysis and generation, text processing and generation, or defeating people at human-developed games. As highlighted in the 2023 Department of Defense (DoD) Data, Analytics, and Artificial Intelligence Adoption Strategy, AI is essential to the DoD mission. Moreover, recent global conflicts have demonstrated the utility of emerging AI-enabled battlefield systems, as they can help improve the speed, quality, and accuracy of decisions in the field, providing a decisive warfighting advantage.

Despite recent rapid advancements in AI that have the potential to transform DoD warfighting, there has been significant research at the intersection of computer security and AI that demonstrates the brittleness of AI models. The nature of AI models makes them prone to unknown natural and deliberately induced errors that could be exploited. Prior work in this space has demonstrated vulnerabilities of AI models in a wide variety of AI attacks, such as test time attacks, data poisoning, and forensic attacks, which extract model and training data information. These attacks can lead to several downstream AI effects, such as reduced model performance, the embedding of malicious backdoor behavior, and the extraction of potentially sensitive information on the dataset used for training. These prior works have highlighted potentially core vulnerabilities and may reduce DoD willingness to adopt AI-based solutions.

However, most of the aforementioned AI attack effects have been primarily demonstrated in controlled settings that offer pristine control of input/training data and unrestricted access to model components, which may mislead the efficacy of these attacks in a DoD operational setting.

For instance, in most prior work, the notion of access, or how model weights are obtained, as well as the vector used to deliver an AI attack effect, are abstracted away. Prior research often assumes direct access to the inputs of a model and full white box access to model weights for the generation of the AI attack effect. In a practical application of an AI attack effect, we must consider the nuances of an AI-enabled system deployed in a DoD setting. In DoD settings, AI models are developed in system pipelines that ingest and curate data from multimodal sensors, update AI models, orchestrate deployment to a server or on a device, which then takes in information from a sensor in dynamic real-world operating conditions to be processed by the model. This pipeline has several avenues that an adversary may seek to gain access (Figure 1); however, the utilization of these AI attack vectors in conjunction with AI attacks to create a downstream AI attack effect has seen limited study. To understand the risk of deploying an AI-enabled system in this setting, exploration must be done as to how an adversary may utilize these (and potentially other) vulnerabilities to cause an AI attack effect or exfiltrate useful knowledge that could support a future attack.

As another example, prior work generally disregards the dynamics of operationally gathered sensor data. That work considers single instances of data over which the attacker will have pristine control. However, pristine control of input data to a system is not a viable assumption in DoD settings. For example, in the case of observational image data, one must consider the variety of lighting/weather conditions, movement of both the observer and the observed resulting in changes in distance and view angle, sensor specific processing, and physical transferability of a developed attack. To understand the risk of deploying an AI-enabled system given the operational dynamics, the AI attack vectors must be used/developed with consideration for and then tested within these operational dynamics.

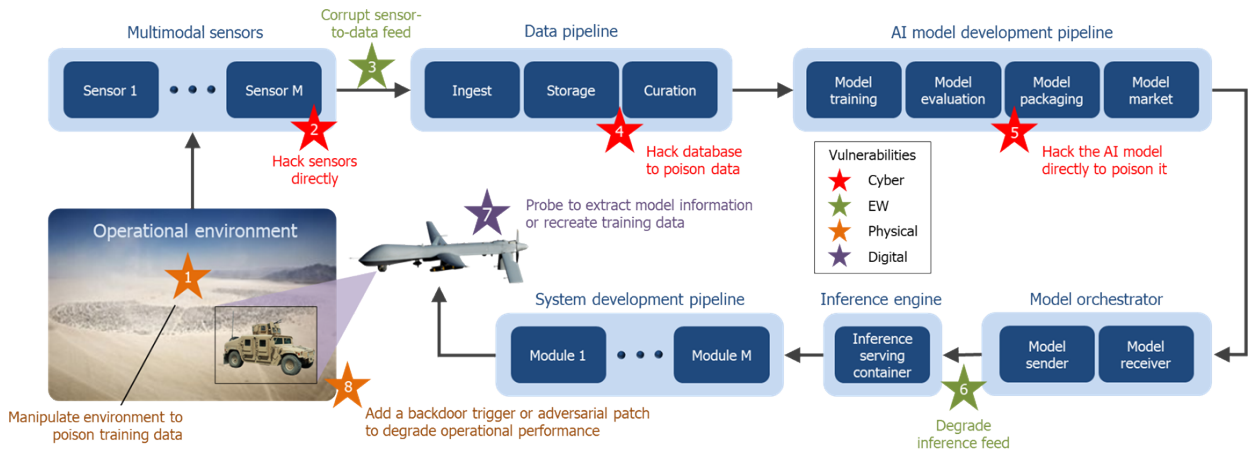

Figure 1: Example of an AI-enabled battlefield system development/deployment pipeline of a multi-sensor drone, containing an AI object detection model, for aerial target identification where possible vulnerabilities are identified.

The above discussion serves to highlight that even though previous research work gives a large upper bound on the effectiveness of AI attack effects, it is still an open question as to whether these effects will reach that upper bound in practice. The next step is to discern the practical operational

risks that a deployed AI-enabled system brings to the battlefield through extensive AI security OT&E.

The DoD uses well-established guidelines and processes for cybersecurity OT&E; however, the same cannot be said for AI security OT&E, i.e. operational AI red teaming. As of today, there is no well-developed capability and broader ecosystem that operationally assesses deployed military AI-enabled battlefield systems for vulnerability to AI attack effects. Further, there are no techniques/tools that would enable an AI red team to carry out an AI attack effect over numerous potential threat vectors, nor exemplar AI kill chain TTPs for how to assess these systems.

SABER aims to establish a replicable exemplar for AI security OT&E through the development of counter-AI techniques, tools, and processes that will create and execute novel AI kill chains that enact an AI attack effect. Our exemplar will be proved through a series of operationally realistic AI security OT&E exercises (SABER-OpX), setting the blueprint for how future assessments should be conducted, over diverse AI tasks of interest to the DoD.

Program Introduction

SABER will conduct operationally realistic AI security OT&E exercises, herein referred to as SABER-OpX, that will catalyze an operational AI red teaming ecosystem of technology, processes, places, and people necessary to secure AI-enabled battlefield systems for warfighter use. SABER-OpX participants will consist of three technical teams (TTs). TT1 will be comprised of ***SABER Research Performers*** who will survey, evaluate, select, develop, employ, and integrate counter-AI techniques/tools in two separate research foci, AI Attack Effect Techniques/Tools (TT1.1), or Toolkit Integration (TT1.2). TT2 will be comprised of existing DARPA & Government Research Performers (GRP). TT3 will be comprised of a Government Team tasked with design, setup, execution, and evaluation of the SABER-OpX exercises. ***Note***, this solicitation is ***only*** soliciting abstracts and proposals for ***TT1 SABER Research Performers,*** more specifically TT1.1 (AI attack effect techniques/tools) and TT1.2 (Toolkit Integration). TT2 and TT3 information is provided to explain the construction and anticipated execution of the SABER program. Abstracts and proposals received in response to TT2 or TT3 will not be considered for award.

Program Structure

The following is a description of the Program Structure, specifically a broad description of SABER-OpX participants, a description of SABER-OpX exercises, and a more in-depth description of SABER Research Performers (TT1).

(1) **SABER-OpX Participants**

Technical Team 1 – SABER Research Performers (Soliciting for submissions):

Technical Team 1.1 (TT1.1): Support the AI red team through the survey, evaluation, selection, development, and use of AI attack effect techniques and red teaming tools.

Technical Team 1.2 (TT1.2): Support integration and employment of these AI attack effects and red teaming tools. Develop an operational AI red teaming framework and toolkit.

Technical Team 2 – Research Participant (Information Only):

Technical Team 2 (TT2): Provide access and use of their existing AI-enabled battlefield systems and support experimentation for operational assessments.

Technical Team 3 – Government Participant (Information Only):

Technical Team 3 (TT3): May be comprised of University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), National Laboratories, and Government Subject Mater Experts.

Utilizing the output of SABER Research Performers (TT1), TT3 will 1) research and develop counter-AI techniques/tools alongside TT1 performers, 2) develop novel AI kill chain TTPs and employ selected and integrated counter-AI techniques/tools developed by TT1, 3) provide feedback on utility and suggestions for improvement to TT1, and 3) assess/measure the operational impact/risk of AI attack effects on a target ASUT within a SABER-OpX.

Furthermore, TT3 will be responsible for planning and logistics support for each SABER-OpX and compiling the developed TTPs and lessons learned for further dissemination in support of technology transition.

(2) SABER-OpX Exercises

SABER-OpX will be a series of **two** AI security OT&E exercises based on realistic operational scenarios that highlight DoD tasks (e.g., Intelligence, Surveillance, and Reconnaissance, autonomy, AI Target recognition, etc.) in a contested space, with platforms such as AI-enabled autonomous ground vehicles and rotary-wing drones. SABER-OpX exercises will red team recently developed AI-enabled battlefield systems designed for operational use and attempt to estimate the operational impact/risk of performance degradation of an adversary exploiting AI model and pipeline vulnerabilities to degrade operational effectiveness.

Each SABER-OpX will be operational in nature, meaning that to the highest fidelity possible, experimentation will attempt to mimic the dynamic conditions that may influence a system while in use, including an instance of an AI pipeline for model (re)training. TT3 may manipulate the entirety of the AI pipeline, which includes the operational environment, sensor feeds, data pipelines, AI model development pipelines, model orchestrators, inference engines, etc. (see Figure 1). However, system access will not be given a priori: no credentials will be provided for accessing a database, no backdoors will be pre-installed on sensors, no model weights will be disseminated prior to attack, etc. Further, the operational environment itself at inference-time may provide challenges that limit the efficacy of AI assessed only in laboratory conditions. As an example, an adversarial patch naively placed in a field must contend with a variety of physical constraints, such as view angle to sensor, ambient lighting conditions, weather, glare, etc.

Given the above, TT3 will need a variety of counter-AI techniques and tools to probe various potential AI attack vectors to deliver AI attack effects. These may include "physical" effects (to manipulate the operational environment to further manipulate sensor feeds), "cyber" effects (to gain access across the AI pipeline, sensors, databases, models, etc., and extract information about the system), and/or "EW" effects (to corrupt sensor data or inference feeds or degrade base system functions).

Each SABER-OpX will focus primarily on near-term discriminative (not generative) AI-enabled battlefield systems that will be provided directly by TT2. SABER-OpX #1 will focus on AI-enabled ground autonomy, with the TT3 seeking to reduce the overall speed of an autonomous ground vehicle navigating to a goal position. SABER-OpX #2 will focus on AI-enabled rotary wing drone-based aerial autonomy, with TT3 seeking to reduce the success rate of these drones accomplishing their autonomous missions (e.g., recon, strike). Each of these platforms will have their own suite of sensors. Ground autonomy will likely have optical, thermal, global positioning system, Light Detection and Ranging (LiDAR), and radio detection and ranging (RADAR) as data input sources, whereas the aerial autonomy will likely only have optical and thermal sensors. Moreover, each AI-enabled battlefield system will have its own accompanying AI infrastructure for AI-based perception enabling the autonomy, which may also present vulnerabilities for attack.

Each SABER-OpX exercise will be a nine-month series of four experiments with events occurring in months one, three, six, and nine. The month one experiment will be an opportunity for TT3 to gather baseline results, utilizing only existing techniques/tools and TTPs to operationally assess the ASUT. Experiments at months three, six, and nine will employ the techniques/tools developed/integrated by SABER Research Performers (TT1). Further schedule details can be found in the subsequent section, (5) Program Schedule.

(3) SABER Research Performers (soliciting for submissions)

As noted in Section III, Program Structure Technical Team 1 (TT1) is made up of SABER Research Performers. TT1 is broken out into TT1.1 AI Attack Effect Techniques/Tools and TT1.2 into Toolkit Integration. DARPA anticipates multiple awards for TT1.1 and a single award for TT1.2. Prime proposers may submit a single abstract/proposal in response to TT1.1 **or** TT1.2, but **not** both. Potential subcontractors may only team with one prime proposer for a single team submission.

TT1.1: AI Attack Effect Techniques/Tools

TT1.1 submissions should focus on the development and application of techniques/tools to enable an AI attack effect (versus a cyber/EW attack effect). AI attack effects can be achieved through cyber/EW attack vectors (cyber/EW attacks on the AI components of the system pipeline) or AI attack vectors (AI-informed attacks on the AI components of the system pipeline). As discussed previously, SABER broadly characterizes these AI attack vectors as PACE methods. This categorization is not exhaustive, and DARPA welcomes well-reasoned submissions that do not fit neatly within these categories.

Traditional and/or AI-assisted cyber/EW attack vectors may be used to directly cause an effect on the AI components of the systems or to extract system information that may be used to aid in the execution of another attack vector. However, for the purposes of these experiments it will be out-of-scope to directly manipulate components down-stream of the AI components of the system.

Examples:

- The use of cyber means to extract AI model weights embedded on a system to improve other downstream AI attack effects is IN SCOPE.
- The use of cyber means to manipulate model weights/sensor input to manipulate the steering of an autonomous system is IN SCOPE.
- Directly manipulating the steering of an autonomous ground systems without attacking AI components is OUT OF SCOPE.

Whether proposing a technique to enable AI attack effects via physical, adversarial AI, cyber, EW, or other AI attack vectors, proposers will be required to describe a concept of operation (CONOP) indicating how the proposed technology could be used to enable an AI attack effect.

Example:

- Consider there is a data store utilized in (re)training of autonomy perception models. A method for infiltrating the data store could be used to manipulate training data, enacting a data poisoning attack that would reduce the performance of the AI model in a particular environment, while still performing well on test ranges.
- For physical vectors, a glare resistant printing material with high RGB pixel fidelity could be used to develop more resilient adversarial patches. The specific design may have properties that enable rapid deployment in a potentially contested space.
- For EW, emissive methods could be used to manipulate sensors over multiple spectra in subtle ways as to enable perturbation style adversarial attacks.

In writing this CONOP, consider how proposed method(s) will impact the measured quantities of the AI Red Team Effectiveness Metric (ARTE, see *(Table 2) Program Metric*): performance, cost, and time. In addressing performance, justify the benefits of utilizing your attack vector compared to others. In terms of cost, highlight the expected cost of the implementation of your attack, and why that cost might be justified. In terms of time, consider the time to deploy an attack through your vector, justifying their appropriateness given the constraints of an operational environment.

Strong TT1.1 abstracts and proposals should demonstrate:

- Experience in the development/implementation of practical counter-AI techniques, particularly with reduced access threat models, such as gray, black, and hidden box methods.
- Exquisite, targeted technologies in a domain that will enable successful implementation of AI attack effects. These technologies are diverse; however, useful components include technologies for high quality printing/manufacturing, light projection, offensive cyber, EW, as well as others.

- A CONOP, documenting how your technology will enable an adversarial AI attack effect against an AI-enabled battlefield system pipeline and justifying its operational utility.
- A strong team of developers who can interface with TT1.2/Government for employment.

TT1.2: Toolkit Integration

Given the diversity of counter-AI techniques and tools within the scope of TT1.1 and to ensure that TT3 can efficiently explore the space of attack vectors/effects, TT1.2 will be responsible for development and integration of TT1.1 techniques into a unified operational AI red teaming framework. That framework should enable a seamless generation of AI attack effects through the attack vector techniques and tools surveyed, evaluated, selected, and developed in TT1.1.

A unified framework should be capable of:

1) incorporating AI attack effects emerging from TT3 and
2) incorporating knowledge of the operational environment and ASUT to generate AI attack effects that are informed by the down-stream AI attack vectors developed by TT1.1.

TT1.2 teams will need to work closely with TT1.1 and TT3 to augment existing adversarial attacks. Thus, TT1.2 will need to ensure that AI attack effects generated through the unified framework are resilient to both the dynamics of the operational environment and lose minimal effectiveness when translating through the attack vector. AI attack effects may require the development of novel methods of AI attack effect generation that consider the AI attack vector and the operational dynamics. The unified framework should also consider that the level of knowledge for the AI pipeline component under attack may be low and should be able to incorporate information as it is made available to improve the success of the overall AI attack effect.

Strong TT1.2 abstracts and proposals should demonstrate:

- Experience in the development/implementation of practical AI attack effects, particularly over reduced access threat models, such as gray, black, and hidden box models.
- The ability to contribute novel methods of AI attack effects that account for the dynamics of an operational environment, as well as a particular AI attack vector for the adversarial attack. Experience in solving more traditional Sim-to-Real problems in AI may also be a strength.
- Experience in the development of AI-enabled systems for deployment in real world settings.
- Experience in developing toolkits via the integration of other techniques/tools.
- Excellent software engineering practices pulling together various systems originally un-intended to work together.

Program Metric

SABER program success will be measured by developing AI attack effects that maximize the ARTE metric, which is defined as:

$$\square\square\square\square = 1/(\square_{\square}\square + \square_{\square}\square + \square_{\square}\square)$$

where:

- *P*, a ratio of the performance measure of an AI-enabled system when an AI attack effect is applied (causing degradation) to the performance measure of an AI-enabled system without the application of an AI attack effect (no adversarial degradation)
- *T*, time (normalized) to generate and deliver the AI attack effect
- *C*, cost (normalized) to generate and deliver the AI attack effect
- θ_i, a set of importance weights that will balance each measured quality with respect to the operational setting of the evaluation

Note that P is a ratio between zero and one. To allow for appropriate comparison, *T* and *C*, maximum time and cost, respectively, will be normalized to fall within this range. The procedure for normalization will be determined based on the results of baseline experimentation in each SABER-OpX.

The ARTE metric is designed to elicit a trade-space of viable solutions, rather than a single solution for a given problem. Additionally, the metric is designed to be flexible as informed by the operational context for each SABER-OpX. Note that this metric is a value that more directly measures the performance of TT3. Thus, SABER Research Performers will be measured by an increase in the overall ARTE value captured within SABER-OpX #1 experiment one. DARPA expects this value to increase over the course of SABER-OpX experiments, as presented below:

SABER-OpX 1 & 2	Percent Increase in ARTE
Month 1	BASELINE
Month 3	10% increase in BASELINE
Month 6	20% increase in BASELINE
Month 9	40% increase in BASELINE

Table 2: Expected increase over SABER-OpX experiments.

The above metric targets are the same for each SABER-OpX experiment. However, the $\square_{\square}$ values may change between SABER-OpX 1 and 2 based on the operational use of the different ASUTs in SABER-OpX 1 and 2.

Program Schedule

As depicted in Figure 2, SABER consists of a single 24-month program with four key stages. Months 1-4 will be allotted for initial development and SABER-OpX preparations. SABER-OpX #1 exercise will span months 5-13, while SABER-OpX #2 exercise will span months 14-

22. Each exercise will consist of four separate week-long experiments. Months 23-24 will be a "cool down" period, focusing primarily on packaging final deliverables for transition and holding a final meeting to encapsulate the program effort and discuss potential next steps based on the program results.

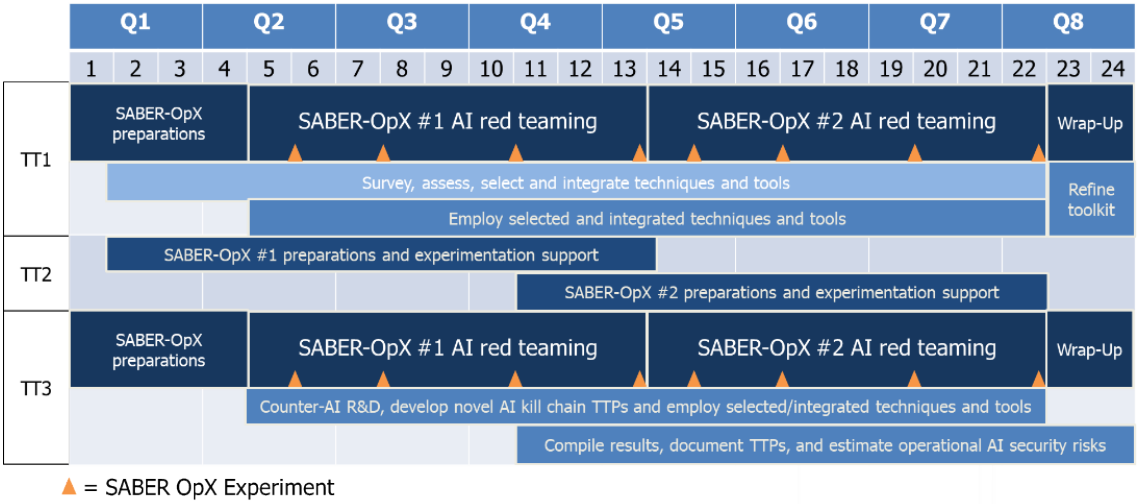

Figure 2: SABER program schedule.

Proposers should plan and budget key technical personnel (prime and subcontractor) attendance at the following events:

1. One kick-off meeting in month one;
2. Eight SABER-OpX experiment events; and,
3. One wrap-up meeting in month 23.

Note, proposers may assume both the kick-off and wrap-up meetings will be held in Arlington, VA for one day each. Additionally, proposers should anticipate budgeting travel for four trips to Seattle, Washington, and four trips to West Point, NY for SABER-OpX experiments. Proposers should ensure budgets reflect sufficient funds for key technical personnel who will most directly contribute to on-site task adjustments and support for utilization of TT1 tools. Proposers may budget for additional personnel to attend the meetings and events if the proposer can demonstrate the value the program will receive from the person(s)' attendance.

Additionally, proposers (prime and subcontractor) who plan to propose travel for conferences should describe why attendance at the conference(s) will benefit the project and how the proposer will mitigate cost and schedule impacts to the SABER program.

SECTION IV: EVALUATION CRITERIA

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

- **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. The proposed technical approach builds on prior mature technology and/or expertise in frontier research areas applicable to the program. 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.

- **Potential Contribution and Relevance to the DARPA Mission:** The potential contributions of the proposed effort bolster the national security technology base and support DARPA's mission to make pivotal early technology investments that create technological surprise for national security. The proposer clearly demonstrates its capability to transition the technology to the research, industrial, and/or operational military communities in such a way as to enhance U.S. defense. In addition, the evaluation will take into consideration the extent to which the proposed intellectual property rights structure will impact the Government's ability to transition the technology.

- **Cost and Schedule Realism:** The proposed costs are representative of the proposer's scope of work and reflect a sufficient understanding of the costs and level of effort needed to successfully accomplish the proposed technical approach. The proposed costs for the prime and team (subcontractors, consultants, etc.) are substantiated by supporting documentation and/or details that allow the Government to discern cost realism. 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. It is expected that the effort will leverage all available relevant prior research to obtain the maximum benefit from the available funding. 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 to be in a more competitive posture. DARPA discourages such cost strategies.

Unless otherwise specified in this announcement, for additional information on how DARPA reviews and evaluates proposals through the Scientific Review Process, please visit: Proposer Instructions and General Terms and Conditions

SECTION V: SECURITY REQUIREMENTS

At this time, DARPA anticipates that proposals submitted in response to this BAA may generate or involve access to classified information. Classified submissions shall be transmitted and marked in accordance with the following guidance.

Potential proposers are strongly encouraged to request the SABER Security Classification Guide (SCG) to carefully review the SABER classification guidance, prior to preparing any abstract/proposal material. The SABER SCG is CUI and will be transmitted to eligible proposers via the Department of Defense Secure Access File Exchange (DoDSAFE).

The SABER SCG will only be released to eligible organizations that request it by emailing the below outlined information to SABER@darpa.mil with the title "[org name] SCG request". All information must be received no later than March 31, 2025, at 5PM ET in a complete and accurate manner for DARPA to consider requests for the SCG.

No later than April 24, 2025, proposers intending on preparing classified proposal material must request a DD Form 254, "DoD Contract Security Classification Specification" and be issued a DD-254 for HR001125S0009 prior to starting work on any classified proposal materials. DARPA anticipates issuing solicitation DD-254s by May 1, 2025. DD-254 requests will be emailed to SABER@darpa.mil with the title "[org name] DD-254 request" and follow the format below. All information must be received in a complete and accurate manner for DARPA to consider requests to issue a DD-254.

SCG and Classified Proposal Request Format:

1. Organization's Legal name:
2. CAGE Code:
3. Physical address:
4. Email address to receive the SCG:
5. Screenshot or pdf copy of the requesting organization's Supplier Performance Risk System (SPRS) risk score or Cybersecurity Maturity Model Certification CMMC assessment.
6. Highest classification of material to be included in the proposal:

NOTE: The prime proposers shall not further disseminate the SCG to subcontractor team members without verifying the recipient's information technology systems meet the requirements outlined for Controlled Unclassified Information (CUI) on Non-DoD Information Systems found here: https://www.darpa.mil/about/offices/contracts-management/proposer-general-terms.

Security Eligibility Criteria

DARPA anticipates SABER work will be performed at the unclassified, CUI, and SECRET levels. The prime proposer organization must be a U.S organization able to receive, process, and store classified information at the SECRET level. Proposals must demonstrate the following in the capabilities section of Volume I (Technical and Management).

Prime proposal team members are required to satisfy the following requirements to be eligible for selection:

- At least 3 U.S. citizen key management personnel with minimum final SECRET clearances. Successful proposals will demonstrate that a sufficient number of technical staff have SECRET clearances in addition to key personnel.
- A plan to ensure a sufficient number of locations on the proposal team possess a Defense Counterintelligence and Security Agency (DCSA) SECRET facility clearance letter (FCL) with SECRET safeguarding within 90 days of contract award.
- Demonstrate the ability to obtain DCSA accreditation of a SECRET collateral information system with sufficient computing to support any proposed SECRET work within 90 days of contract award.

CUI Submissions

Unclassified submissions containing CUI may be submitted via the DARPA Broad Agency Announcement Tool (BAAT). 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 https://www.darpa.mil/about/offices/contracts-management/proposer-general-terms

Classified Submission Requirements and Procedures

Classified submissions shall be transmitted and marked in accordance with the DARPA SABER SCG, which will be provided upon request, in accordance with the instructions previously stated.

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

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

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

Submissions containing both classified information and CUI must be appropriately and conspicuously marked with the proposed classification level, as well as ensuring CUI is marked in accordance with DoDI 5200.48.

Classified Submissions

For classified abstract/proposals, proposers will ensure all industrial, personnel, and information systems processing security requirements are in place and at the appropriate level (e.g., Facility Clearance Level (FCL), Automated Information Security (AIS), Certification and Accreditation (C&A), and any Foreign Ownership Control and Influence (FOCI) issues are mitigated prior to submission. Additional information on these subjects can be found at https://www.dcsa.mil/.

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

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

Confidential and Secret

- Notification of intent to submit classified proposal material via one of these means must be sent to SABER@darpa.mil no later than April 24, 2025, or the classified proposal material may not be considered. Confidential and Secret classified information may be submitted via one of the following methods or transmitted via the means for Top Secret:

  - Hand-carried by an appropriately cleared and authorized courier to the DARPA Classified Document Registry (CDR). Prior to traveling, the courier shall contact the DARPA CDR at 703-526-4052 to coordinate arrival and delivery.

  OR

  - Mailed via U.S. Postal Service (USPS) Registered Mail or USPS Express Mail. All classified information will be enclosed in opaque inner and outer covers and double-wrapped. The inner envelope shall be sealed and plainly marked with the assigned classification and addresses of both sender and addressee. Senders should mail to the mailing address listed in the contact information herein.

  - The inner envelope shall be addressed to Defense Advanced Research Projects Agency, ATTN: I2O BAA HR001125S0009.

  - The outer envelope shall be sealed with no identification as to the classification of its contents and addressed to Defense Advanced Research Projects Agency, Security & Intelligence Directorate, Attn: CDR.

  OR

- Emailed via DoD Secret Internet Protocol Router Network (SIPRNET) or DARPA Secret Wide Area Network (DSWAN), with prior notification to SABER@darpa.mil.

Top Secret Information

Notification of intent to submit classified proposal material via these means must be sent to SABER@darpa.mil no later than April 24, 2025, or the classified proposal material may not be considered:

Top Secret information must be hand-carried by an appropriately cleared and authorized courier to the DARPA CDR. Prior to traveling, the courier shall contact the DARPA CDR at 703-526-4052 to coordinate arrival and delivery.

Alternatively, Top Secret information may be transmitted to DARPA via Joint Worldwide Intelligence Communications System (JWICS) email, DoD Secure Integration Cloud (SIC) or the DARPA Savannah Ascend Network.

Pertinent Information at other Classification Levels: Abstract/proposals may incorporate prior work or data at the SCI level or at Special Access Program (SAP) levels. SAP information must be marked in accordance with DoDM 5205.07 Volume 4 and transmitted by specifically approved methods, which will be provided by the Technical Office BAAO or their staff. Proposers choosing to submit SAP information from an agency other than DARPA are required to provide the DARPA Technical Office Program Security Officer (PSO) written permission from the source material's cognizant Special Access Program Control Officer (SAPCO) or designated representative. For clarification regarding this process, contact the DARPA Technical Office PSO via the BAA mailbox or the DARPA SAPCO at 703-526-4102.

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

NOTE: *All abstract/proposals containing SAP information must be processed on a SAP information technology (SAP IT) system that has received an Approval-to-Operate (ATO) from the DARPA Technology Office BAAO or other applicable DARPA SAP IT Authorizing Official. The SAP IT system ATO will be based upon the Risk Management Framework (RMF) process outlined in the Joint Special Access Program Implementation Guide (JSIG), current version (or successor document). (Note: A SAP IT system is any SAP IT system that requires an ATO. It can range from a single laptop/tablet up to a local and wide area networks.)*

The Department of Defense mandates the use of a component's SAP enterprise system unless a compelling reason exists to use a non-enterprise system. The DARPA Chief Information Officer (CIO) must approve any performer abstract/proposal to acquire, build, and operate a non-enterprise SAP IT system during the awarded period of

performance. Use of the DARPA SAP enterprise system, SAVANNAH, does not require CIO approval.

SAP IT disposition procedures must be approved in accordance with the DoD CIO Memorandum of April 20, 2020.

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 can be submitted through the DARPA Broad Agency Announcement Tool (BAAT). The classified portion must be provided separately, according to the instructions outlined in the 'Classified Submission Requirements and Procedures' section above.

SECTION VI: ABSTRACT GUIDELINES

This announcement contains an abstract phase. Proposers are strongly encouraged to submit an abstract in advance of a full proposal submission to minimize effort and reduce the potential expense of preparing an out-of-scope proposal; however, submission of an abstract is not required.

Abstract Content

Abstract content and formatting requirements are stated in the Abstract Instructions and Submission Template and the Abstract Summary Slide Template found in the Abstract Attachments (A-1 and A-2). All abstracts submitted in response to this solicitation must comply with the content and formatting requirements stated in the aforementioned attachments. Use of the Abstract Templates is ***required*** in development of abstract submissions. Information not explicitly requested in this solicitation and the abstract attachments may not be reviewed.

Abstract Submission Requirements:

- The Abstract submission deadline is as stated in Section I: Overview Information.
- Abstracts must be submitted to the DARPA Broad Agency Announcement Tool (BAAT). Please visit Proposer Instructions and General Terms and Conditions for specific information regarding submission methods through BAAT. Submissions sent through other mediums, channels, or after the prescribed deadline will not be accepted.
- Proposers are responsible for clearly identifying proprietary information on the Abstract cover page. Marking must state, "Proprietary." Note, "confidential" is not 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.

Abstract Feedback:

- DARPA will review abstracts for conformance; only conforming abstracts will be reviewed and receive feedback.
- All conforming abstracts will receive written feedback either encouraging or discouraging a full proposal submission. The Government's feedback determination will be accompanied by a brief technical analysis which resulted in the feedback response. Feedback will be sent to the administrative and technical points of contact noted in the abstract cover page.
- Regardless of DARPA's response to an abstract, proposers may submit a full proposal. Without regard to any comments or feedback resulting from the review of an abstract, DARPA will review all conforming full proposals using the published evaluation criteria.

SECTION VII: PROPOSAL GUIDELINES

Proposal Preparation Requirements

All proposers must be registered in the System for Award Management (SAM) and have a Unique Entity Identifier (UEI) number for their proposal to be found conforming. Proposers must maintain an active registration in SAM.gov with current information at all times during which a proposal is under consideration or have a current award with DARPA. Information on SAM registration is available at SAM.gov.

NOTE: New registration takes an average of 7-10 business days to process in SAM.gov. Registration requires at a minimum the following information:

- SAM UIE number.
- Tax Identification Number.
- Commercial and Government Entity (CAGE) Code. If a proposer does not already have a CAGE code, one will be assigned during the SAM registration process.
- Electronic Funds Transfer information (e.g., proposer's bank account number, routing number, and bank phone or fax number).

Proposal Content

This announcement allows for multiple award instrument types to include Procurement Contracts and Other Transactions. Some award instrument types have specific cost-sharing requirements. All proposals submitted in response to this announcement must comply with the content and formatting requirements stated in the Proposal Attachments. Proposers are ***required*** to use the templates provided; information not explicitly requested in this announcement or the Attachments, may not be evaluated.

Procurement Contracts: Proposer Instructions: Procurement Contracts
Other Transaction Agreements: Proposer Instructions: Other Transactions

SECTION VIII: SUBMISSION INFORMATION

- This announcement allows for multiple award instrument types, to include Procurement Contracts and Other Transactions. Some award instrument types have specific cost-sharing requirements. The following websites are incorporated by reference and contain additional information regarding overall proposer instructions, general terms and conditions, and each specific award instrument type.

  - **Proposer Instructions and General Terms and Conditions**: Proposer Instructions and General Terms and Conditions
  - **Procurement Contracts**: Proposer Instructions: Procurement Contracts
  - **Other Transaction agreements**: Proposer Instructions: Other Transactions

- This announcement contains an abstract phase. Abstracts are strongly encouraged but not required. Abstracts are due on the date and time stated in Section I, Overview. Additional instructions for abstract submission are contained within the **Abstract Attachments.**

  Abstract Attachments:
  - **(required) A-1** Abstract Summary Slide Template
  - **(required) A-2** Abstract Instructions and Template

- Full proposals are due on the date and time stated in Section I, Overview. The **Proposal Attachments** contain specific instructions and templates and constitute a full proposal submission. Please visit Proposer Instructions and General Terms and Conditions for specific information regarding submission methods through the Broad Agency Announcement Tool (BAAT).

  Proposal Attachments:
  - **(required) P1:** Proposal Summary Slide Template
  - **(required) P2:** Proposal Instructions and Volume I Template (Technical and Management)
  - **(required) P3:** Proposal Instructions and Volume II Template (Cost)
  - **(required) P4:** DARPA Standard Cost Proposal Spreadsheet

- Baseline Model Contracts and Other Transactions are attached to this solicitation. Redline edits to the corresponding Baseline Model should be submitted with the proposal.

  Baseline Model Contracts
  - Baseline Model-Contract Large Business
  - Baseline Model-Contract Small Business
  - Baseline Model-Contract Addendum Circumstance-Driven Additional Clauses
  - Baseline Model-OT P-Fixed Support Nontraditional
  - Baseline Model-OT R-Fixed Support Company

SECTION IX: SPECIAL CONSIDERATIONS

- This announcement, stated attachments, and websites incorporated by reference constitute the entire solicitation. In the event of a discrepancy between the announcement, attachments, or websites, the announcement shall take precedence.

- Non-U.S. organizations and/or individuals cannot participate in this solicitation. All other responsible sources capable of satisfying the Government's needs may submit a proposal that shall be considered by DARPA. Historically Black Colleges and Universities, Small Businesses, Small Disadvantaged Businesses and Minority Institutions are encouraged to submit proposals and join others in submitting proposals; however, no portion of this announcement will be set aside for these organizations' participation due to the impracticality of reserving discrete or severable areas of this research for exclusive competition among these entities.

- At this time, DARPA anticipates that abstract/proposals submitted in response to this BAA may generate or involve access to classified information. See Section V for more information.

- DARPA has utilized an alternate structured approach for the determination of a reasonable fee basis for Cost-Plus-Fixed-Fee (CPFF) procurement contracts under SABER, in accordance with DFARS 215.404-4(b)(1)(C). The fee calculation percentage range determined reasonable for procurement contract awards under SABER is 8.6% - 9.6%. This was determined based on consideration of factors such as: performance risk; contract type risk; facilities capital employed; anticipated award size; available transition path; markets (commercial, Government, international); IP rights; chances of award; time to production; and solicitation complexity. Proposers should propose a fee that falls within the above range. Because that fee range already has been determined to be reasonable relative to SABER, proposals need not include any further fee justification. Elimination of fee as a negotiation item is expected to result in reduced contracting timelines for any proposal selected for award negotiation. It should be noted that this structured approach may not apply to other transactions requested by nontraditional defense contractors.

- DARPA encourages technical solutions from all responsible sources capable of satisfying the government's needs. To ensure fair competition across the ecosystem, DARPA prohibits contractors/performers from concurrently providing Systems Engineering Technical Assistance (SETA), Advisory and Assistance Services (A&AS), or similar support services and being a technical performer, unless the DARPA Deputy Director grants a written waiver. DARPA extends this prohibition to University-Affiliated Research Centers (UARCs) and Federally Funded Research and Development Centers (FFRDCs) including National Labs, who as a result of their specialized expertise and areas of competencies, are able to accomplish integral tasks that cannot be met by government or contractor resources. Therefore, these entities are highly discouraged from proposing against this solicitation as award to a UARC or FFRDC will only be made by exception. UARCs and FFRDCs interested in this solicitation, either as a prime or a subcontractor, should contact the Agency Point of Contact (POC) listed in the Overview section prior to the proposal (or abstract) due date to discuss potential participation as part of the government team or eligibility as a technical performer.

- As of the date of publication of this solicitation, the Government expects that program goals as described herein either cannot be met by proposers intending to perform fundamental research or the proposed research is anticipated to present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Therefore, the Government anticipates restrictions on the resultant research that will require the awardee to seek DARPA permission before publishing any information or results relative to the program. For additional information on fundamental research, please visit Proposer Instructions and General Terms and Conditions.

- DARPA is interested in whether, and to what extent, proposers are using artificial intelligence (AI) tools to contribute to Volume 1 of proposals submitted in response to DARPA solicitations. Therefore, proposers must answer the following questions on the cover sheet of Volume 1 of this solicitation: o 1) Did you use AI tools to assist in preparing this proposal? o 2) If yes, what tools did you employ? Any content in Volume 1 that utilized an AI tool to generate information, assist in technical understanding, or guide the technical work should have a citation and a corresponding reference in the Bibliography section of Volume 1. The citation should specify the tool, content, and purpose. For example, "[AI tool] was used to understand existing state-of-the-art in manufacturing." NOTE – THIS INFORMATION WILL NOT BE USED FOR EVALUATION PURPOSES. Proposals will be evaluated in accordance with the Evaluation Criteria outlined in the solicitation regardless of whether AI tools were employed.

- The APEX Accelerators program, formerly known as the Procurement Technical Assistance Program (PTAP), focuses on building strong, sustainable, and resilient U.S. supply chains by assisting a wide range of businesses that pursue and perform under contracts with the DoD, other federal agencies, state and local governments, and with government prime contractors. See https://www.apexaccelerators.us/ for more information. APEX Accelerators helps businesses:
    - Complete registration with a wide range of databases necessary for them to participate in the government marketplace (e.g., SAM).
    - Identify which agencies and offices may need their products or services and how connect with buying agencies and offices.
    - Determine whether they are ready for government opportunities and how to position themselves to succeed.
    - Navigate solicitations and potential funding opportunities.
    - Receive notifications of government contract opportunities on a regular basis.
    - Network with buying officers, prime contractors, and other businesses.
    - Resolve performance issues and prepare for audit, only if the service is needed, after receiving an award.

- Project Spectrum is a nonprofit effort funded by the DoD Office of Small Business Programs to help educate the Defense Industrial Base (DIB) on compliance. Project Spectrum is vendor-neutral and available to assist businesses with their cybersecurity and compliance needs. Their mission is to improve cybersecurity readiness, resilience, and compliance for small/medium-sized businesses and the federal manufacturing supply chain. Project Spectrum events and

programs will enhance awareness of cybersecurity threats within the manufacturing, research and development, as well as knowledge-based services sectors of the industrial base. Project Spectrum will leverage strategic partnerships within and outside of the DoD to accelerate the overall cybersecurity compliance of the DIB.

www.Projectspectrum.io is a web portal that will provide resources, such as individualized dashboards, a marketplace, and Pilot Program to help accelerate cybersecurity compliance.

- DARPAConnect offers free resources to potential performers to help them navigate DARPA, including "Understanding DARPA Award Vehicles and Solicitations," "Making the Most of Proposers Days," and "Tips for DARPA Proposal Success." Join DARPAConnect at www.DARPAConnect.us to leverage on-demand learning and networking resources.

- DARPA has streamlined our Broad Agency Announcements and is interested in your feedback on this new format. Please send any comments to DARPAsolicitations@darpa.mil.