THIS IS A SOURCES SOUGHT NOTICE ONLY. This Sources Sought Notice is a means of obtaining feedback from contractors concerning the requirements stated in Sections 3 and 4, which is part of the acquisition planning and market research phase for this procurement.

The industry input received from this Sources Sought Notice will aid in determining available sources that can meet the Government's below stated requirements and may be considered in the preparation of the official solicitation package.

This Sources Sought Notice does not constitute a solicitation.

The anticipated NAICS for this requirement is 541690 "Other Scientific and Technical Consulting Services". If contractors believe a more appropriate NAICS applies to the requirement as detailed below, include the feedback in your response.

SUBJECT: Sources Sought Notice HR001126QE005 for DARPA Program Security Services

1. INTRODUCTION

The Defense Advanced Research Projects Agency (DARPA) is conducting this Sources Sought to identify contractors who possess the capabilities to provide Program Security Services, as specified herein, and to determine their availability and capability.

If your firm may be interested in this requirement and has performed similar projects, we request the information shown below. All business sizes under the applicable NAICS should consider submitting a response to this notice.

As permitted by Federal Acquisition Regulation (FAR) Part 10, this is a market research tool being utilized for informational and planning purposes. Your responses will assist the Government in the development of its acquisition strategy for a possible Request for Quote (RFQ) or Request for Proposal (RFP), to be issued at a later date, and in determining whether there are contractors capable of completing the requirements utilizing a General Services Administration (GSA) Contract Vehicle.

To facilitate market research, the Government is seeking to identify qualified sources to perform Program Security Services, as specified in the subsequent sections of this Sources Sought Notice. The Government is requesting responses from Small Businesses and Other than Small Businesses to assess if there is a qualified vendor pool capable of performing the required services, as well as determining if there are any opportunities for Small Business set-asides and participation. The Government will analyze all responses to determine the pool of qualified firms and any small business set-aside/participation opportunities.

This notice shall not be construed as an RFQ, RFP, or as any commitment or obligation on the part of the Government to issue a solicitation. The Government does not intend to award a contract based on this request, so quotes **will not** be considered.

No reimbursement will be made for any costs associated with providing information in response to this synopsis or any follow-up information requests.

Response is strictly voluntary – it is not mandatory to submit a response to this notice to participate in any formal solicitation process that may take place in the future. However, it should be noted that information gathered through this notice may significantly influence our acquisition strategy.

2. SECURITY AND INTELLIGENCE DIRECTORATE (SID) BACKGROUND AND MISSION.

DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise by sponsoring revolutionary, high-payoff research and development projects. This implies one imperative – radical innovation for national security. DARPA's business philosophy is to bring in expert, entrepreneurial Program Managers (PMs) for the technical programs, empower them, protect them from red tape, and enable them to quickly make decisions about starting, continuing, or stopping research projects. The DARPA technical staff organization is dynamic and changes as the projected requirements of the Department of War (DoW), the state of technology development, and adversarial threats evolve. To support this unique program management approach, The DARPA, Security & Intelligence Directorate (SID) requires Program Security personnel to serve as that are as expert in their own field as the PMs are in theirs.

The Security & Intelligence Directorate (SID) supports the DARPA mission through a proactive and flexible organization led by a small cadre of government security professionals supported by contractor subject matter experts. These services require personnel who can apply risk-managed, proactive program protection and related security services to the broad range of DARPA research & development projects at the fundamental research, controlled unclassified, collateral, special accesses program (SAP), and sensitive compartmented information (SCI) levels. These personnel must be subject matter experts across multiple security disciplines, must not be paralyzed by the unknown or unfamiliar, and must possess critical thinking and analytical problem-solving skills that foster the creation of innovative security solutions to support program timelines and objectives, while maintaining compliance with applicable national security requirements.

3. DESCRIPTION OF THE REQUIREMENT.

The SID Program Security Services requires a unique set of expertise that goes well beyond traditional security disciplines such as Physical Security, Personnel Security, Information & Industrial Security, and International Security. The preponderance of the work includes services provided by Program Security Representatives (PSRs). PSRs are embedded directly into the DARPA Technical Offices as part of a DARPA PM's team; they are the "tip of the spear" for execution of SID's primary function, enabling the secure development of DARPA technologies. Many DARPA projects involve more than one level of classification and/or SAP compartmentation, as well as frequently informed by or have transition activities that involve Controlled Access Programs (CAPs), GAMMA sub-compartments, Sensitive Source Reporting Programs (SSRPs), or Alternative Compensatory Control Measures (ACCMs). Due to this broad range and combination of classification/compartmentation, DARPA requires PSRs that have a sound understanding of the numerous security policies and procedures associated with these types of information, as well as expert ability to develop and implement security architectures for technology spanning this spectrum.

3.1. Anticipated Period of Performance: The anticipated period of performance is detailed in the table below with an estimated start date beginning in the second quarter of fiscal year 2027.

Base Period	**12 Months**
Option Period One (1)	**12 Months**
Option Period Two (2)	**12 Months**
Option Period Three (3)	**12 Months**
Option Period Four (4)	**12 Months**

3.2. Contract Type: The Government anticipates issuing a single-award, Cost-Type or Time and Materials, Task Order.

3.3. Government Estimated Level of Effort: The Government anticipates this effort requiring approximately 160 Full Time Equivalent contractor personnel.

4. <u>SCOPE.</u> The scope of work includes:

4.1. Analyze and create program protection strategies and tactics, frequently for technologies that exist nowhere else.

4.2. Development of program security objectives, to include:

4.2.1. Identification of critical and enabling technologies through the Technology Decomposition process;

4.2.2. Determining applicable national security policy and existing related programs for horizontal protection; facilitating intelligence and counterintelligence support;

4.2.3. Projecting test and transportation security needs; and intelligently crafting and executing proposed security classification architectures and program protection plans that balance security requirements with program cost and schedule constraints.

4.2.4. PSRs must also consider and address a program's post-DARPA acquisition life cycle to ensure that security does not become an impediment during program transition to a Service or Agency partner.

4.2.5. Providing contract and operations management support providing recruitment and retention of high-quality personnel, ensuring proper accounting, inventory, purchase, and disposition of government-furnished equipment and other consumable materials, and overseeing the submission of quality deliverables. This also includes monitoring and managing the security contract and contractors as well as supporting the Director SID/SAPCO, DD/SID, and DD/SAPCO.

4.2.6. Providing security support to DARPA leadership, including the Director, Deputy Director, Chief of Staff, and Military Service Liaisons, in their classified activities managing DARPA programs and operations, coordinating with DoW civilian and military leadership, as well as providing technical advice and status updates on DARPA programs to senior Executive Branch and Legislative Branch appointed and elected officials.

4.2.7. Maintaining a Countering Foreign Intelligence Program (CFIP) that focuses on fundamental research security for DARPA grants and other funded activities, providing analysis of individuals and entities who propose to DARPA projects, and creating risk assessments associated with the research and/or the proposer.

4.2.8. Maintaining an Insider Threat capability to correlate, analyze, and organize various data streams, triggers, and anomalous behaviors in order to provide SID leadership with insider threat baselines, items of interest, and focus issues.

4.3. Providing a Program Information Technology (PIT) Security Controls Assessor (SCA) capability for PIT systems at all classification levels, supporting technology areas such as:

4.3.1. Space systems,
4.3.2. Manned and unmanned aircraft systems,
4.3.3. Manned and unmanned surface/sub-surface vessels,
4.3.4. Cyber weapons development and operational platforms,
4.3.5. Weapons data links,
4.3.6. RF communications systems,
4.3.7. Directed energy systems,
4.3.8. Portable electronic devices for battlefield use.

4.4. Maintaining an archival system for current and completed DARPA classified projects, ensuring compliance with Information Security Oversight Office, National Archives and Records Administration, and DoW historical recording keeping, declassification, and file series exemption requirements.

4.5. Providing database administration/web development and technical support for a variety of SID

database/data management systems to record, track, organize, and utilize information related to various SID functions, to include SAP management, oversight, and administration.

4.6. Supporting the Director and Deputy Director, SAPCO in the administration of the DARPA SAP portfolio as well as their responsibilities for ACCM and CAP activities.

4.7. Providing a service/capability to destroy SAP IT equipment in accordance with current DoW standards.

4.8. Providing Counterintelligence (CI) Analyst support possessing subject matter expertise in a broad spectrum of CI areas to support DARPA's programs and program managers. This includes, but is not limited to, researching and collecting required data, perform analyses, and summarize findings in response to customer requests; working with individual program management personnel to assist in analyzing and developing solutions to unique or difficult CI-related issues; and providing threat data and analyses to support technology assessments.

4.9. Providing Senior Technology Analysts who will utilize all-source intelligence analyst skills to access and analyze information on state of the world technology to inform leadership decisions on initial technology investment and development pathways related to U.S. capabilities. Responsibilities may include establishing system access requirements and procedures designed to inform on specific technologies, both foreign and domestic. The analyst will also identify risk and vulnerability to any potential investment or programmatic pursuit.

4.10. Maintaining policy oversight by providing security policy interpretation, application, advice, and assistance to the DoW, IC, or defense industry.

4.11. Providing an Information and Industrial Security support team to perform activities including, but not limited to: Special Security Agreements, Voting Trusts, Proxy Agreements, DD 254 Contract Security Classification Specifications, National Interest Determinations (NIDs), Manual Declassification review processes, Classified Document Registry, and Security Compliance Inspections.

4.12. Maintaining an International Security Team to assist the program security representatives in the exchange of information with foreign nationals, managing and complying with treaty compliance issues, assisting with export control matters, analyzing Foreign Ownership, Control, or Influence (FOCI) cases, and other International Security matters.

4.13. Providing a Personnel Security team to manage the DARPA Badge Office, Common Access Card Office, Clearance Processing Center, and Special Security Office.

4.14. Providing a Security Education and Training Awareness Specialist responsible for developing and delivering DARPA's security education products and newcomer orientation materials and briefings.

4.15. Creating, developing, coordinating, and managing program protection strategies to support DARPA programs and technology thrust areas via a Science and Technology Protection Analysis team.

4.16. Providing a Cybersecurity Cross Domain Solutions (CDS) SCA capability responsible for conducting comprehensive security assessments of CDSs operating at various classification levels.

4.17. Providing a team of Security Administrators responsible for maintaining information within databases that reflect receipt, storage, inventory, and disposition of information including data entry, updates, and generation of reports as well as personnel security accesses, to include databases for SAP and SCI personnel, and conduct indoctrination and debriefings as required.

4.18. Providing a Technical Security Support Specialist team to maintain numerous database/data management systems to record, track, organize, and utilize information related to SAP compartments/sub-compartments, SAP facilities, information, briefed personnel, and other pertinent data associated with SAP management, oversight, and administration.

5. SUBMISSION REQUIREMENTS

All interested contractors certified small business concerns (please specify which type(s)) or other than small business concerns, who believe they can meet the requirements described in this Sources Sought Notice are invited to submit, in writing, complete information describing their ability to provide the deliverables under this effort.

5.1. Submission Due Date: All questions and responses shall be submitted to the Contracting Officer, via e-mail, on or before **5:00 PM Eastern Time on July 24, 2026**. The Contracting Officer's contact information is listed below:

Contracting Officer: Dr. Alexis Shellow
Email: programsecurityrequirement@darpa.mil
SUBJECT LINE: Sources Sought HR001126QE005 DARPA Program Security Services

5.2. Submission Format: Submissions to this Sources Sought shall be submitted:

5.2.1. Using Microsoft Word or Adobe PDF format
5.2.2. Using 12-point Times New Roman Font
5.2.3. Using 8.5 x 11-inch page size

6. PAGE LIMITATION: Submissions shall adhere to the following page limitations:

Item	Title	Page Limitation
1	Coversheet	1 Page
2	Attachment 1 (Sections 1 and 2) - Experience Reference Information	1 Page/Reference
	Attachment 1 (Section 3)- Experience Reference Narrative	1 Page/Reference
3	Attachment 2 - Requirement Feedback	N/A
	Attachment 2 - OCI Intent to Participate	N/A

The total page count for each submission to this Sources Sought Notice shall not exceed five (5) pages, not to include Attachment 2.

7. SUBMISSION CONTENT. Interested firms should submit their response to include the following (in this order):

7.1. Item 1: Coversheet. Please submit a coversheet that includes the following information:

7.1.1. Complete business name
7.1.2. Unique Entity Identifier (UEI)
7.1.3. Commercial and Government Entity (CAGE) Code
7.1.4. Contact information (POC's name and title, address, telephone, email)
7.1.5. Business size and classification (e.g., Small, SBA Certified 8(a), HUBZone, Service-Disabled Veteran-Owned) under NAICS code 541690
7.1.6. List of GSA Schedules and/or other Multiple Award contract vehicles (if any) that interested party has been awarded and can be utilized for this requirement (e.g. GSA OASIS+)

7.2. **<u>Item 2: Attachment 1 Experience Reference Sheet.</u>** Please provide the following information using Attachment 1- Experience Reference Sheet and ensure the following information is included. Please submit no more than two (2) Experience References. For each reference, the narrative section shall not exceed one page per reference.

7.2.1. Confirmation of the ability to meet the Security Requirements identified in Section 8.
7.2.2. Identification of current or prior contracts for which you have provided program security services that are similar in size and scope of this requirement, and description of how those services would enable you to fulfill DARPA requirements outlined in this Sources Sought Notice.
7.2.3. Limited to the past five (5) years
7.2.4. Any government contract examples must include contract numbers, project titles, dollar amounts (total value and average funded value per year), number of full-time equivalents (FTE) provided, periods of performance, and Government POCs (telephone and email)

7.3. **<u>Item 3: Requirement Feedback and Conflict of Interest Determination.</u>** Please provide the following information using Attachment 2.
7.3.1. Feedback on the following as the Government develops its requirement:
7.3.2. Does your firm have a DCAA-approved cost accounting system?
7.3.3. If your firm cannot fulfill all the requirements on its own, do you have a teaming partner identified? If so, what firm(s)?
7.3.4. What additional information would you need from the Government to be able to provide an accurate proposal
7.3.5. Identification of any potential Organizational Conflicts of Interest
7.3.6. Probability (high, medium, or low) of participating in a solicitation for a requirement derived from this Sources Sought Notice.

8. <u>SECURITY REQUIREMENTS.</u>

The Contractor, and any subcontractors, must possess a Top-Secret Facility Clearance. All individuals supporting this contract must possess, at the time of assignment, a Top Secret personnel security clearance, based on a Tier 5 or Tier 5R Background Investigation, current within five (5) years, and adjudicated for SCI eligibility by an authorized Central Adjudication Facility. Individuals outside the 5-year scope, but entered into Continuous Evaluation with a deferred investigation, meet this requirement.

9. <u>DISCLOSURES</u>

Respondents are advised that DARPA is under no obligation to acknowledge receipt of the information received or provide feedback to respondents with respect to any information submitted under this notice. Responses to this notice do not bind DARPA to any further actions, to include directly requesting proposals from organizations responding to this notice.

Submissions may be reviewed by the Government (DARPA and partners) and Scientific Engineering and Technical Assistance (SETA) contractors. All personnel with access to the submissions will be covered by a legally-binding non-disclosure agreement.

NO CLASSIFIED INFORMATION SHOULD BE INCLUDED IN SOURCES SOUGHT NOTICE RESPONSES.