REQUEST FOR INFORMATION / SOURCES SOUGHT NOTICE
(BIAO-RFI-2026)

Title: Basic Information Awareness Operations (BIAO)

Notice Type: Request for Information (RFI)/Sources Sought Notice

Agency: Strategic Capabilities Office (SCO)

1. Background

The ability to operate effectively in the information environment is a critical component of national security. This environment is increasingly contested. Adversaries conduct cognitive domain operations (CDO) or 'cognitive warfare', which involves coordinated influence activity executed at machine speed and scale, across digital media platforms to shape how populations perceive, sense-make, and act. The cost of generating and propagating synthetic and manipulated content continues to fall while the volume and sophistication continue to rise, outpacing human-speed review and detection.

The Strategic Capabilities Office (SCO) is pursuing Basic Information Awareness Operations (BIAO), a rapid prototyping effort to deliver a layered, modular capability to detect adversary CDO, generate and deliver counter-narrative responses with accurate information, model and validate effectiveness, and deploy and measure outcomes in operationally relevant settings. SCO intends to acquire capability on a technology-component basis and to integrate those components into a single, scalable operating environment — referred to notionally as the Layered Information Nexus (LIN), which will serve as the common operational picture and workbench — for use across a broad operational user base.

2. Description of Requirement

This is an RFI/Sources Sought Notice issued by SCO for informational and planning purposes only. SCO is conducting market research to identify traditional and non-traditional sources capable of providing all or any portions of these technology components, and, separately, sources capable of serving as the integrator of those components. SCO is interested in conducting a rapid prototyping effort with feasible transition paths and is interested in demonstrating capability as quickly as possible.

Although not an immediate requirement for this RFI/Sources Sough Notice, the Government is highly interested in sources possessing or having a clear path to obtaining the appropriate facility and personnel security clearances to work on controlled and, where applicable, classified information systems and subsystems.

Response Tracks

SCO is seeking information across two distinct response tracks. Interested parties must clearly indicate, at the front of their submission, which track they are responding to:

- **Track A – Technology Component Developer:** Interested parties offering capabilities that satisfy all or any portion of one or more of the technology components described below.
- **Track B – Integrator:** Interested parties offering capabilities to integrate the technology components into a single, scalable operating environment (the LIN), conduct data management, and to deliver that environment to operational users.

Organizational Conflict of Interest (OCI)

To prevent an Organizational Conflict of Interest (OCI), the Government intends to strictly separate the integrator role from the component development role. The selected Integrator (Track B) will not be permitted to develop or supply the underlying technology components (Track A). Interested parties must clearly indicate whether they are submitting for Track A, Track B, or both. While an organization may submit capabilities for both tracks, it cannot be selected for both.

Foundational Principle: Open Architecture & Modularity

All proposed solutions, regardless of the specific technology component, must be built on an open architecture utilizing common, well-documented interface definitions (e.g., REST APIs, standard data formats). The primary goal of this effort is to establish a multi-vendor, plug-and-play environment. Consequently, proprietary "black box" systems that create vendor lock-in or hinder seamless integration are not aligned with the Government's objectives.

Track A – Technology Components

SCO seeks capabilities that satisfy all or any portion of the following technology components. Interested parties need not address an entire component; best-in-class capability addressing a single function or sub-function is welcome. The Government highly values existing and deployed capabilities.

Technology Component 1 – Detection

- **Objective:** SCO is seeking innovative capabilities for detecting adversary cognitive domain operations across the global information environment. Detection may include capabilities to ingest, parse, and analyze multi-platform data feeds to identify, track, and alert on emerging adversary narrative campaigns, coordinated inauthentic behavior (CIB), and synthetic/manipulated media.
- **Areas of Interest:** Interested parties should describe their technical approach, methodologies, and any existing technologies for addressing the following areas:
  - **Coordinated Inauthentic Behaviors:** Detecting adversarial influence campaigns across single vs. multi-platforms and single vs. multiple personas; identifying region of influence and origination.
  - **Manipulated Content:** Detection of AI-generated or manipulated content (images, video, audio, text) and deepfakes.
  - **Agent Activity:** Detecting coordinated agents, their scale, and amplification methods; providing virality ratings; conducting metadata curation and checking; applying geo-fencing;

Key Questions for Industry: Submissions should detail how the proposed solution achieves these detection outcomes and should address the following questions.:

- Does your capability rely on its own organic data dependencies, or is it designed to process data feeds provided by a separate integration platform?
- What other aspects or emerging capabilities in cognitive warfare detection should the Government consider for this requirement?
- What methodologies and metrics are recommended for the Government to conduct a technical evaluation of detection capabilities, ensuring the delivery of best-in-class solutions to operational users?"

Technology Component 2 – Generation

- **Objective:** SCO is seeking innovative and mature capabilities to rapidly generate and prepare tailored counter-narratives and multi-modal assets for operational deployment.
- **Areas of Interest: Interested parties** should describe their technical approach, methodologies, and any existing technologies for addressing the following areas:
  - **Counter-Narrative Generation:** Generating robust counter-narratives; determining what content resonates with specific audiences; and assessing the optimal method, speed, and region of delivery, including projecting virality.
  - **Integration with Modeling & Simulation (M&S):** Architecting generation workflows to seamlessly export proposed counter-narratives and multi-modal assets into the M&S environment for verification, validation, and efficacy testing prior to operational deployment.
  - **Team-of-Agents Construction:** Building and managing teams of agents (e.g., Large Language Models vs. Small Language Models) with human-on-the-loop (HOTL) oversight for coherent, multi-media content delivery.
  - **Response Readiness:** Creating "response cards" (shovel-ready, metric-informed content) to enable rapid and pre-approved counter-messaging.
  - **Digital Twins & Fine-Tuned Agents:** Developing and utilizing "digital twins" or fine-tuned AI agents to ensure high-fidelity, persona-accurate, and rapid message generation for strategic communications.
- **Key Question for Industry:** Submissions should detail how the proposed solution generates these assets and should address the following questions:
  - How does your solution generate these assets while maintaining message integrity and operational safety through human-in-the-loop workflows?
  - How would your component ingest threat alerts and audience parameters from an external system and push the finished response assets into a central repository for deployment?
  - How is your generation capability designed to interoperate with a M&S environment to allow for rapid, iterative testing and validation of assets before they are deployed?
  - What level of robustness and analysis is done within your component for each item generated?
  - What methodologies are recommended for the Government to conduct a technical evaluation of generation capabilities, ensuring the best-in-class solutions are delivered to the users?

Technology Component 3 – Modeling & Simulation / Verification & Validation (M&S/V&V)

- **Objective:** SCO seeks innovative and mature capabilities to simulate, model, and validate the potential efficacy of both adversary campaigns (simulated or derived) and proposed counter-narratives prior to operational deployment.
- **Areas of Interest:** Interested parties should describe their technical approach, methodologies, and any existing technologies for addressing the following areas:
  - **Modeling & Simulation Environments:** Building and managing M&S environments, including the use of population models, regional characteristics, personas, points of origination, and predicted effectiveness ratings.
  - **Validation & Verification (V&V):** Conducting network analysis, topological validation, and behavioral alignment (e.g., using Bayesian methods or other models); generating similarity and viability scores for networks and narratives.
  - **Metrics & Analytics:** Defining, capturing, and analyzing key metrics within the simulation, including network metrics, message virality, speed to deliver, delivery medium effectiveness, and pattern-of-life / behavior tracking to identify and assess cognitive operations.

- **Key Question for Industry:** Submissions should address the following questions:
  - How do your modeling and wargaming system(s) handle highly dynamic, unpredictable human environments and data scarcity?
  - How would your component ingest counter-narratives and audience profiles, execute the simulation, and output quantitative scores to inform operational decision-making?
  - What methodologies are recommended for the Government to conduct a technical evaluation of M&S capabilities, ensuring the delivery of best-in-class solutions to operational users?

Technology Component 4 – Deploy & Measure (Deploy/MOEs)

- **Objective:** SCO is seeking innovative and mature capabilities to execute the operational deployment of approved counter-narratives and to measure their digital and physical effectiveness in real-time.
- **Areas of Interest:** Interested parties should describe their technical approach, methodologies, and any existing technologies for addressing the following areas.
  - **Capability Deployment & Integration:** Ensuring the technology is containerized and architected for rapid execution at both the edge and on global networks.
  - **Digital Measures of Effectiveness (MOEs):** Developing and tracking novel digital MOEs that go beyond traditional social media engagement or virality metrics to assess deeper cognitive impact.
  - **Physical Measures of Effectiveness (MOEs):** Methodologies to quantify the real-world impact and physical outcomes of digital generated content.
  - **Feedback Mechanism:** Establishing a robust feedback loop to continuously provide performance data back into the system to refine active and future operations.
- **Key Question for Industry**: Submissions should address the following questions:
  - What is your methodology for measuring effectiveness, particularly how you propose to attribute physical-world outcomes to digital information campaigns? How would your component deliver metrics to inform an operational picture?
  - Describe the ability for your capability to ingest externally generated campaigns and narratives for deployment.
  - How would you recommend the Government conduct technical evaluations of deployment and measuring capabilities to ensure best in class solutions are delivered to the users?

Track B – Integrator Opportunity

- **Objective:** SCO is seeking a highly capable systems integrator to architect, build, and maintain the Layered Information Nexus (LIN). The LIN is the secure, scalable, and modular backbone of the BIAO system. The Integrator will ensure interoperability among diverse Track A technology components and deliver unified user experience.
- **Areas of Interest:** Interested parties should describe their technical approach, methodologies, and relevant experience in addressing the following critical integration functions:
  - **Architecture & Common Data Schema:** Designing and implementing an open, API-first architecture; defining and managing a unified data schema that standardizes inputs and outputs across various multi-modal data streams and specialized vendor tools.

- **Secure Hosting & Compliance:** Establishing and managing a secure cloud hosting environment capable of operating at DoD Impact Levels 5 and 6 (IL5/IL6); ensuring continuous monitoring and compliance with DoD cybersecurity frameworks (e.g., RMF, DevSecOps pipelines).
- **Integration Middleware (APIs/SDKs):** Developing, documenting, and maintaining robust Application Programming Interfaces (APIs) and Software Development Kits (SDKs) to facilitate the rapid, "plug-and-play" integration of third-party Track A components (Detect, Generate, Model, Deploy).
- **Common Operational Picture (COP)/User Interface**: Designing, developing, and iterating on the user-facing dashboard or "workbench." This interface must intuitively fuse outputs from multiple Track A components into a single, cohesive view for operators to analyze threats, generate responses, wargame outcomes, and measure effectiveness. Potential exists to integrate this unified UI into a larger enterprise solution.
- **Data Ingestion & Management:** Providing robust data management and routing architectures; addressing whether the LIN will ingest raw data feeds directly to distribute to Track A components, or if it will primarily serve as a routing hub for processed data from those components.
- **Data Acquisition & Sourcing:** The Integrator must demonstrate the capability to identify, procure, and integrate diverse data sets which could include both government and commercial sources to support Track A technology components.

- **Key Question for Industry:** Submission should address the following questions:
  - What is your approach to managing “vendor lock”? What is your methodology for integrating components from Track A vendors into a seamless interface?
  - What methodologies are recommended for the Government to conduct a technical evaluation of integrator capabilities, ensuring the delivery of best-in-class solutions to operational users?

Unlisted or Emerging Capabilities

The technology components described above represent the Government’s current understanding of the BIAO functional architecture. However, SCO acknowledges that the pace of technological change is rapid. Interested parties possessing a mature or emerging capability relevant to the BIAO mission which may not align with one of the four components are strongly encouraged to submit it for consideration. Submissions must clearly label this section as "Unlisted Capability.”

3. Objectives

The objectives of this RFI/Sources Sought Notice are to:

1. Conduct Market Research to Understand the Art of the Possible:

- Identify a diverse range of industry sources—including small/large and traditional/non-traditional businesses—capable of fulfilling the technology component developer (Track A) or integrator (Track B) roles.
- Understand the technical maturity, commercial availability, and architectural modularity of existing dual-use capabilities relevant to the BIAO mission.
- Assess the current industrial base capacity regarding cleared personnel and secure facilities available to support work on controlled and classified systems.

2. Refine the BIAO Acquisition Strategy:

- Inform Government decisions regarding prototyping, evaluation criteria, and the overall acquisition approach for a rapid, component-based program.
- Obtain direct industry feedback on the contemplated acquisition strategy, including the use of SCO's authority to award an Other Transaction (OT) for Prototype under 10 U.S.C. § 4022, a six-month continuous on-ramp/off-ramp cadence, and the proposed Organizational Conflict of Interest (OCI) mitigation structure.

3. Identify and Mitigate Programmatic Risks:

- Identify major technical, programmatic, and integration risks as perceived by industry experts.
- Assess the feasibility of robust small business participation at both the component and integration levels.

4. Submission Instructions

Interested parties are requested to submit a White Paper responding to the criteria below. Submissions should be organized into the following sections. Where an item does not apply to the selected response track, the responder should explicitly state this.

Part 1: Administrative & Executive Summary (All interested parties)

- **Response Track Declaration:** At the very top of the first page, clearly state whether your submission is for Track A (Technology Component Developer) or Track B (Integrator).
- **Entity Information:** Full legal name, mailing address, CAGE/NCAGE Code, Unique Entity ID (UEI), business size standard per applicable NAICS, socio-economic classifications, and whether the company is foreign owned.
- **Point of Contact (POC):** Name, title, email address, and phone number for the primary technical POC.
- **Executive Summary (1-2 pages recommended):** Briefly describe the proposed solution, the unique value proposition, the maturity of the technology (TRL), and relevant past performance or independent testing results.

Part 2: Detailed Capability Description (Track-Specific)

- **For Track A:** Identify the addressed components (1, 2, 3, or 4). Describe technical approach, open architecture modularity (APIs, data formats), and answer the Key Questions for Industry posed in Section 2.
- **For Track B:** Describe integration approach (architecture, data schema, COP development, workflow management). Explain the organizational approach to maintaining strict OCI separation while managing component subcontractors and answer the Key Questions for Industry posed in Section 2.

Part 3: Security & Export Controls (All interested parties)

- State Facility Clearance Level (FCL) and clear personnel count. Identify any Export Administration Regulations (EAR) and/or International Traffic in Arms (ITAR) restrictions. List relevant existing or past government contract(s) or OT award(s), both for Research (10 U.S.C. § 4021) and for

Prototype (10 U.S.C. § 4022). Existing Government contracts/awards and/or FCL is not a prerequisite for response to this RFI/Sources Sought Notice.

Part 4: Acquisition Strategy Feedback (All interested parties)

- Provide recommendations/critiques on the component-based model with an OCI-restricted integrator, use of Other Transaction authority, six-month continuous competition cadence, and the strategy for protecting proprietary data.
- Describe the standard commercial pricing and licensing model (e.g., enterprise license, per-user SaaS, consumption-based API) utilized for the proposed capability and provide recommendations on how to scale that model for a Department of War (DoW) enterprise deployment.
- **Recommended NAICS Code(s):** If applicable to your organization, recommend the most appropriate primary NAICS code and explain how it impacts the organization's ability to propose or team.
- **Missing Components:** Identify any capabilities, subcomponents, or strategic considerations omitted from this RFI/Sources Sought Notice.

Part 5: Optional Video Demonstration

- Interested parties may optionally include a secure, accessible hyperlink within their White Paper to a narrated technical demonstration video of their capability.
- Videos must focus on technical workflow and user interfaces; generic corporate marketing or promotional videos are prohibited.
- Videos shall not exceed 8 minutes in length.

5. Formatting & Proprietary Guidelines

- **Document Format:** The White Paper shall be submitted as a single PDF file, font size minimum of 10-point, not to exceed ten pages (excluding the cover page). If proposing multiple technology components or tracks, an additional two pages is granted per additional TC and/or track. The file size shall not exceed 15MB.
- **File Naming Convention:** Submissions must be saved and sent using the following file naming format: BIAO_RFI_[Track]_[Company Name].pdf
    - Example for Track A: BIAO_RFI_TrackA_ABCCorp.pdf
    - Example for Track B: BIAO_RFI_TrackB_ABCCorp.pdf
    - Example for Both Tracks: BIAO_RFI_TracksAB_ABCCorp.pdf
- **Disclaimer:** This RFI/Sources Sought Notice is issued solely for informational, market research, and planning purposes. It does not constitute a Request for Proposal (RFP) or Request for Quotation (RFQ). The Government will not accept proposals or pay for any costs incurred in responding to this notice.
- **Proprietary Information:** Interested parties must clearly mark any proprietary information. Each page containing proprietary information must be marked "PROPRIETARY" at both the header and footer. The Government shall not be liable for the disclosure of any proprietary information not properly identified. Submissions may be reviewed by Government support contractors bound by non-disclosure agreements (NDAs).

6. Submission Logistics & Inquiries

- **Submission Email:** All responses must be sent via email to: BIAO@sco.mil
- **Email Subject Line:** The subject line must follow this exact format: *BIAO RFI Submission – [Company's Full Name] – [Track A or/and Track B]*
- **Submission Deadline:** Responses must be submitted electronically no later than 8:00 PM Eastern/5:00 PM Pacific Time on August 21, 2026.
- **Inquiries:** All questions regarding this RFI/Sources Sought Notice must be submitted via email to BIAO@sco.mil with the subject line: *BIAO RFI Question – [Your Company's Full Name]*. To ensure fair competition, the Government will not answer questions on a one-on-one basis. A consolidated list of all questions and official answers will be posted publicly on SAM.gov on or around August 14, 2026. No new questions will be accepted after 5:00 PM Eastern Time on August 10, 2026.
- The Government may employ analytical and administrative tools, including spreadsheets, databases, document comparison software, search capabilities, and Government-approved artificial intelligence (AI) technologies, to assist reviewers with administrative tasks such as organizing information, identifying references, summarizing submission content, and preparing draft evaluation documentation.