DARPA-BAA-16-34: Enhanced Attribution | Research | USC

DARPA-BAA-16-34: Enhanced Attribution

Slots:
Proposers may only submit one proposal as lead institution to the Enhanced Attribution program. Each proposal may cover one or more technical areas. Proposers may include additional pages for each technical area addressed in the technical approach
LOI: Not mentioned in proposal.
Internal Deadline: **May 6, 2016, 5pm PDT**
External Deadline: **June 7, 2016, 12 pm EST**
Award Information:
Type: Grant
Estimated Number of Awards: Multiple awards are anticipated.
Anticipated Amount: The level of funding for individual awards made under this solicitation has not been predetermined and will depend on the quality of the proposals received and the availability of funds.

Cost Sharing: Cost sharing is not required; however, it will be carefully considered where there is an applicable statutory condition relating to the selected funding instrument.

Submission Process: PIs must submit their application as a *Limited Submission* through the Office of Research Application Portal: https://app.wizehive.com/webform/USCgrants

Materials to submit:

- Single Page Proposal Summary (0.5” margins; single-spaced; font type: Arial, Helvetica, or Georgia typeface; font size: 11 pt.).
- CV – (5 pages maximum)

Link to Award: **https://govtribe.com/project/enhanced-attributionWho May Serve as PI:**
All responsible sources capable of satisfying the Government’s needs may submit a proposal that shall be considered by DARPA. See more information in solicitation regarding eligibility of foreign participation and federally-funded research and development centers (FFRDCs) and government entities.

Purpose:

The program will develop techniques and tools for generating operationally and tactically relevant information about multiple concurrent independent malicious cyber campaigns, each involving several

operators, and the means to share such information with any of a number of interested parties (e.g., as part of a response option). The program seeks to develop:

- technologies to extract behavioral and physical biometrics from a range of devices and vantage points to consistently identify virtual personas and individual malicious cyber operators over time and across different endpoint devices and C2 infrastructures;
- techniques to decompose the software tools and actions of malicious cyber operators into semantically rich and compressed knowledge representations;
- scalable techniques to fuse, manage, and project such ground-truth information over time, toward developing a full historical and current picture of malicious activity;
- algorithms for developing predictive behavioral profiles within the context of cyber campaigns; and
- technologies for validating and perhaps enriching this knowledge base with other sources of data, including public and commercial sources of information.

The Enhanced Attribution program will produce basic technologies and an integrated experimental prototype comprising an end-to-end data collection, fusion, analysis, and validation and enrichment engine.

The program is divided into three technical areas (TA) that will be working in parallel, starting at program kickoff, and will span three 18-month Phases.

TA1: Behavior and Activity Tracking and Summarization – Performers will develop technologies for network behavior and activity tracking and summarization.

TA2: Fusion and Predictive Analysis – Performers will develop technologies for fusion of TA1-generated data and for predictive analysis of malicious cyber operator activities, and will serve as the architect and integrator of the experimental prototype.

TA3: Validation and Enrichment – Performers will focus on validation and enrichment of TA1- collected and TA2-fused data with non-sensitive information (e.g., publicly available data feeds) with the goal of generating a description of the malicious activities using only such data that the Government can publicly reveal in order to expose the actions of individual malicious cyber operators without damaging sources and methods.

Note: Task areas 2 and 3 require a special compartmentalized intelligence facility clearance.
Visit our Institutionally Limited Submission webpage for updates and other announcements.