

IARPA-RFI-14-06

Synopsis

Request for Information (RFI): Cyber Attack Data

The Intelligence Advanced Research Projects Activity (IARPA) is seeking information on data sources for evaluation of cyber attack detection tools and methods. This request for information (RFI) is issued solely for information gathering and planning purposes; this RFI does not constitute a formal solicitation for proposals. The following sections of this announcement contain details of the scope of technical efforts of interest, along with instructions for the submission of responses.

Background & Scope

Cyber attacks are perpetrated by many types of actors, originate from different geographical and logical locations, and utilize various technologies. This RFI seeks to identify existing (non-simulated) data that can be used to evaluate state of the art cyber attack detection techniques in large organizations. Types of data of interest include

- Structured databases that are used to consistently document and report cyber attack events, with minimal latency between report and the cyber event,
- Real-time enterprise data (e.g., host logs, pcap, netflow, security application logs and alerts, help desk ticket details) that cover the period of an event,
- Ground truth data, data suitable for training, and test cases.

Responses to this RFI should answer any or all of the following questions:

- 1) Which existing structured databases consistently document and report cyber attacks? How complete is the coverage, e.g., global, regional, or industry-specific? What is the latency between the cyber attack event and the cyber attack report? Which cyber attack attributes are documented in these databases (e.g., source and target IP range(s), time, intent, indicators of compromise, attacker attribution, victim details, magnitude)?
- 2) What real-time data within an enterprise are most relevant to characterize cyber attacks? How are these data acquired, collected, ingested, encoded, quantified, fused, and/or maintained? Under what terms and conditions would they be deemed sharable with a university/industry research team? How would Personally Identifiable Information (PII) be protected?
- 3) What are appropriate test and evaluation ground truth data, training data, and metrics (e.g., lead time, precision, recall) to measure the performance of automated cyber attack detection systems? Are there good test cases (e.g., from specific industries or organizations) for which data and analyses are available?
- 4) What organizations and/or publications provide base rates for cyber events within different industries? How complete and accurate are they?
- 5) Is there a large organization (> 5,000 users) that would work with a sponsored research program to provide data as a real-world test case? This would require sufficient data

availability so that cyber event detection research systems could be thoroughly exercised and tested. Challenges exist with sharing such data, how might these challenges be overcome?

Preparation Instructions to Respondents

IARPA requests that respondents submit ideas related to this topic for use by the Government in formulating a potential program. IARPA requests that submittals briefly and clearly describe the potential approach or concept, outline critical technical issues/obstacles, describe how the approach may address those issues/obstacles and comment on the expected performance and robustness of the proposed approach. If appropriate, respondents may also choose to provide a non-proprietary rough order of magnitude (ROM) regarding what such approaches might require in terms of funding and other resources for one or more years. This announcement contains all of the information required to submit a response. No additional forms, kits, or other materials are needed.

IARPA appreciates responses from all capable and qualified sources from within and outside of the US. Because IARPA is interested in an integrated approach, responses from teams with complementary areas of expertise are encouraged.

Responses have the following formatting requirements:

1. A one page cover sheet that identifies the title, organization(s), respondent's technical and administrative points of contact - including names, addresses, phone and fax numbers, and email addresses of all co-authors, and clearly indicating its association with RFI-14-06;
2. A substantive, focused, one-half page executive summary;
3. A description (limited to 5 pages in minimum 12 point Times New Roman font, appropriate for single-sided, single-spaced 8.5 by 11 inch paper, with 1-inch margins) of the technical challenges and suggested approach(es);
4. A list of citations (any significant claims or reports of success must be accompanied by citations, and reference material MUST be attached);
5. Optionally, a single overview briefing chart graphically depicting the key ideas.

Submission Instructions to Respondents

Responses to this RFI are due no later than 4:00pm, Local Time, College Park, MD on April 2, 2014. All submissions must be electronically submitted to dni-iarpa-rfi-14-06@iarpa.gov as a PDF document. Inquiries to this RFI must be submitted to dni-iarpa-rfi-14-06@iarpa.gov. Do not send questions with proprietary content. No telephone inquiries will be accepted.

DISCLAIMERS AND IMPORTANT NOTES

This is an RFI issued solely for information and planning purposes and does not constitute a solicitation. Respondents are advised that IARPA is under no obligation to acknowledge receipt of the information received, or provide feedback to respondents with respect to any information submitted under this RFI.

Responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Respondents are solely responsible for all expenses associated with responding to this RFI. IARPA will not provide reimbursement for costs incurred in responding to this RFI. It is the respondent's responsibility to ensure that the submitted material has been approved for public release by the information owner.

The Government does not intend to award a contract on the basis of this RFI or to otherwise pay for the information solicited, nor is the Government obligated to issue a solicitation based on responses received. Neither proprietary nor classified concepts or information should be included in the submittal. Input on technical aspects of the responses may be solicited by IARPA from non-Government consultants/experts who are bound by appropriate non-disclosure requirements.

Contracting Office Address:

Office of the Director of National Intelligence
Intelligence Advanced Research Projects Activity
Washington, District of Columbia 20511
United States

Primary Point of Contact:

Dewey Murdick
Intelligence Advanced Research Projects Activity
dni-iarpa-rfi-14-06@iarpa.gov