

IARPA-RFI-17-04

Synopsis

Request for Information (RFI): Creating a Classified Processing Enclave in the Public Cloud

The Intelligence Advanced Research Projects Activity (IARPA) is seeking information on potential technologies and techniques to securely provide a private enclave encompassing multiple public cloud nodes to accommodate **general-purpose**, classified workloads elastically based on demand. The objective is to accomplish this by replicating as closely as possible the properties of an air-gapped private enclave within the public cloud for finite periods of time.

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

The cost of maintaining and procuring private infrastructure for classified/sensitive workloads for the government continues to get increasingly more expensive compared to the cost of leveraging commercial cloud resources. This disparity may increase exponentially over the next decade. There has been some initial work in the public space attempting to provide more secure computing environments in a commercial cloud. Unfortunately none of these efforts by themselves are currently a viable solution. AMD (SEV), Intel (SGX), Power and ARM processors are introducing some isolation and integrity protection solutions which can isolate certain regions of memory from being read by a general operating system but not from a complicit insider. Fully Homomorphic Encryption (FHE) methods are being developed to perform very specific computations on untrusted platforms but require very high processing overheads and are unlikely to accommodate the entirety of the government's classified codebase. IARPA is interested in developing new technologies and techniques that will enable public cloud owners to provide secure, classified, general purpose processing to the government in an acceptable manner while providing costs and flexibilities comparable to other public cloud customers.

Within this topic, areas of interest include:

- Novel techniques or technologies that can aid in the provisioning of elastic, isolated cloud resources
- Establishing proof of execution of multipurpose scripts on untrusted remote computer systems
- Isolating/disabling computer input/output capabilities temporarily
- Verification techniques to independently ensure computer I/O
- Trusted hardware encryptor technologies that can be employed in servers with customized functionalities
- Performant methods of scrubbing/obfuscating DRAM to prevent cold boot attacks
- Protecting, ensuring, and quickly replacing server and device firmware
- Preventing covert channel communications between two adjacent network servers
- Secure multiparty computational, secret sharing, verifiable computing methods, etc. suitable for protecting or verifying such an environment
- Physically uncloneable functions

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

1. How would you construct a temporary private enclave with future public cloud nodes that could operate all of the software currently found on government classified networks and ensure no data could be leaked either by accident or maliciously?
2. How would you test a private enclave within a public cloud to ensure that no data can leak out?
3. How could a general purpose cloud server be configured to periodically disable and reenable all or most I/O channels?
4. How could one be assured that all I/O paths are verifiably disabled in a server for a certain period of time independent of the server operating system?
5. Can technologies or techniques be employed to ensure that malicious administrators cannot intercept encryption keys or communications between 2 parties even when they control one of the parties?
6. How could a node secure or disable Server Intelligent Platform Management Interface (IPMI) services for brief periods of time?
7. Are there potential solutions for a server to ensure memory used by a private enclave node cannot be revealed when the node is released to the public cloud or when it is seized unexpectedly (cold boot attack)?
8. What methods could be used to ensure remote execution on a particular computer node?

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) estimate 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-17-04;
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);
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 4:00 p.m., Eastern Time, on 19, June 2017. All submissions must be electronically submitted to dni-iarpa-rfi-17-04@iarpa.gov as a PDF document. Inquiries to this

RFI must be submitted to dni-iarpa-rfi-17-04@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 nor 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:

Kerry S. Long
Intelligence Advanced Research Projects Activity
dni-iarpa-rfi-17-04@iarpa.gov