

The Intelligence Advanced Research Projects Activity (IARPA) is seeking information on potential use-cases and associated challenge problems that could be enabled by advanced cryptographic techniques and application development systems facilitating their use, as well as techniques and challenges around building such application development systems.

Use cases of particular interest will be realistic and provide measurable benefits to the intelligence community, other government entities and to the public with respect to automated policy compliance enforcement and verification, and protection of privacy or data in general. Imaginative use cases that currently appear to be infeasible might be enabled by the new technology and cryptographic methods.

Specifically of interest is computing on data belonging to different – potentially mutually distrusting – parties, which are unwilling or unable (e.g., due to laws and regulations) to share this data with each other or with the underlying compute platform. Such computations may include oblivious verification mechanisms to prove the correctness and security of computation without revealing underlying data, sensitive computations, or both.

Responses are also encouraged to highlight challenges to supporting use cases and deploying such 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**

The past decades have witnessed great strides in the development of cryptographic techniques to compute on encrypted or otherwise hidden data, to include fully and partially homomorphic encryption, secure multiparty computation, oblivious RAM, verifiable computation and zero-knowledge proofs. These techniques, if made practical, allow for the ability to securely protect data while under process on computing platforms that cannot be fully trusted, and to collaboratively engage in computations with untrusted parties while obtaining some guarantees as to the integrity of the outputs.

For example, potential use cases include sending private information under encryption to the cloud or to other less trusted parties to have them compute on the data and return answers without ever decrypting or recovering the underlying data, thus reaping significant privacy gains. Other applications include so-called oblivious verification, where certain activities can be verified without revealing related, but sensitive, information – for example, registering an encrypted password with a local system while proving to an external third party that the password follows a particular password policy, without ever revealing the actual password.

While the theoretical cryptography gains have been significant, in practice, implementing cryptographic solutions efficiently and correctly often requires highly specialized knowledge and is extremely difficult. To overcome these issues, IARPA is considering a program, HECTOR, which seeks to facilitate design of highly secure distributed applications and to minimize cryptographic expertise required for these implementations, and will accomplish this by creating a new development stack containing specialized compilers and programming languages, as well as cryptographic libraries implementing both existing

and new/improved protocols. The proposers' day for the HECTOR program is being announced on FBO.gov under IARPA-BAA-17-05.

The goal will be to bring together compiler, programming language, and cryptography researchers to work together on all aspects of the program to create a unified result. This integration is crucial and necessitates research approaches that support a multi-disciplinary effort, including working together to standardize highly technical details in each academic field. For instance, cryptographers will need to work with compiler and programming language researchers to develop a mechanism flexible enough to encompass multiple forms of secure computation, e.g., garbled circuits, homomorphic encryption, oblivious RAM, etc.

IARPA intends to measure the utility of proposed solutions by trying to solve IARPA-furnished challenge problems. An example challenge problem might be to perform various properly authorized statistical analyses on census data without compromising privacy of any individuals (i.e., without revealing to the researchers any data other than the result of the authorized statistical analysis). While some of these sample challenge problems will be furnished to performers at the start of the program, many others will be provided *after* the performers will have been selected, with some of the challenge problems supplied at various stages throughout the program. Therefore, proposed and subsequently developed technical solutions must be highly flexible to address these challenge problems provided after the tools have been developed.

Within this topic, areas of interest include:

- Tools to allow developers to explore the space of distributed applications, and explore composition of different cryptographic techniques, while getting feedback on the feasibility of such applications and compositions given known protocols and the resources they would consume.
- Intuitive programming languages that provide developers with a way to specify the desired security requirements on the one hand, and on the other, able to interoperate with libraries of cryptographic tools, including those developed after the language has been specified (for example, a developer may require ability to verify correctness of the computation – then a verifiable computation protocol may be invoked to provide such a proof of computation's correctness)
- Specification formats and visualization methods for system architecture, security constraints adversarial model and operational environment.
- Compilation techniques for transforming an abstract representation of required secure data services into an intermediate representation consisting of an explicit sequence of calls to functions implementing cryptographic primitives.
- Techniques for automatically generating audit/verification tools for projects that generate an auditable encrypted log, or that provide for cryptographic interrogation of system properties at run-time.
- Development of exemplar applications and responses to challenge problems, using the new programming languages

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

1. Considering advanced cryptographic techniques such as those listed in this RFI, what forms of linguistic expression can concisely and intuitively represent the secure data services being offered to the application by such techniques?
2. What is a particular architectural approach that could be used to allow cryptographic primitives to be invoked automatically by a process that takes into account a specification of the application logic (i.e. application algorithm source code) including the secure data services needed by the application, a specification of the operational environment and adversarial model, and a specification of acceptable algorithms/protocols and security parameters?
3. What is the current state of the art, and challenges for compile-time estimation of the resources consumed (e.g. time, bandwidth, computation, etc.) by an application that invokes a cryptographic protocol or a set of processes that use cryptographic protocols given assumptions (e.g. latency, adversarial model) about the operational environment? To what degree do differences in the number of participants, computation or communication allowance, or security assumptions affect the difficulty or accuracy of such estimation? What types of resources can / should be estimated?
4. To what degree can usability of an application development stack be measured? What approaches are there to quantitatively trade off various usability parameters, as well as potentially other performance or security parameters?
5. What are means to build in verification of an application? Verification could be of inputs, outputs, or of correct computation, and parties requiring verification outputs might be interrogating the system at run-time, or examining generated artifacts after the computation is complete. Parties may also differ significantly in their level access to the underlying data and in the degree and nature of their trust of the involved parties. What are potential challenges to establishing trust in the verification process, and what is the trade-space of mitigations, for example with respect to confidentiality vs transparency?
6. What constitutes a good set of challenge problems, and what are their anticipated degrees of difficulty? What is the trade-space that IARPA should consider to develop challenge problems? This trade-space may focus on the development stack (programming languages, compilers, cryptographic primitives, etc.), but it may also focus on broader issues such as ultimate utility of “solving” the challenge problem.

The responses to this RFI may be used to support a two-day workshop, the tentative date of which is July 12-13, 2017 in the Baltimore/Washington DC area.

Because a limited number of participants is necessary for the intended level of interaction, workshop attendees will be selected based on the quality of responses to this RFI, as well as the government’s need to assemble a range of multi-disciplinary expertise and perspectives.

Representatives of intelligence community, government, policy experts and privacy advocates are encouraged to submit realistic use cases and challenge problems particularly relevant to their organizations. In particular, the policy experts from the intelligence community, other branches of the government and privacy organizations would learn about the potential capabilities that can be enabled by the modern cryptographic and other techniques.

An expected result for such a workshop is the exploration of research challenges in implementing an architecture to seamlessly design cryptographically secure distributed applications as described above,

particularly as they relate to the structure of a potential future IARPA research program in this area.

### **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. 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-17-03;
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 22 June, 2017. All submissions must be electronically submitted to [dni-iarpa-rfi-17-03@iarpa.gov](mailto:dni-iarpa-rfi-17-03@iarpa.gov) as a PDF document. Inquiries to this RFI must be submitted to [dni-iarpa-rfi-17-03@iarpa.gov](mailto:dni-iarpa-rfi-17-03@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. **No proprietary information or classified concepts 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:**

Dr. Mark Heiligman  
Intelligence Advanced Research Projects Activity  
[dni-iarpa-rfi-17-03@iarpa.gov](mailto:dni-iarpa-rfi-17-03@iarpa.gov)