Opportunity Title: Understanding and mitigating side-channels in commodity hardware
Opportunity Reference Code: IC-18-30

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-18-30

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orau.org/icpostdoc/.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 3/12/2018 11:59:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

- Prior academic work has shown side-channels in CPU caches, TLBs, branch predictors, and branch pre-fetchers can be discovered by measuring timing or monitoring debugging features available to software outside the trust boundary. It is less well-understood what other side-channels are exposed by other features of commercially available CPUs or what other properties of computation are measurable for the purpose of side-channel attacks. With increasingly powerful threat models that distrust higher privilege levels, such as those found in protected module architectures or trusted execution environments, more features are exposed to code outside the trust boundary. A deeper understanding of the functional units that contribute to side-channels can lead to ideas about where mitigations should be applied.
- Furthermore, it is not known what mitigations can be applied to existing software to free them of side-channels. Additionally, constructing software that is free of side-channels is a difficult task requiring the use of unusual programming paradigms or programming languages.

Example Approaches:

- Prior academic work has shown side-channels in CPU caches, TLBs, branch predictors, and branch pre-fetchers. A listing of relevant publications can be supplied.
- Research could include detection of side-channels plus strategies to either mitigate them automatically or advise programmers to re-write the

Opportunity Title: Understanding and mitigating side-channels in commodity hardware
Opportunity Reference Code: IC-18-30

code such that it is free of side-channels.

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program.

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12)
  - **Communications and Graphics Design** (6)
  - **Computer, Information, and Data Sciences** (16)
  - **Earth and Geosciences** (21)
  - **Engineering** (27)
  - **Environmental and Marine Sciences** (14)
  - **Life Health and Medical Sciences** (45)
  - **Mathematics and Statistics** (10)
  - **Other Non-Science & Engineering** (5)
  - **Physics** (16)
  - **Science & Engineering-related** (1)
  - **Social and Behavioral Sciences** (28)