Opportunity Title: Quantum secure communication
Opportunity Reference Code: IC-17-35

Organization	Office of the Director of National Intelligence (ODNI)
Reference Code	IC-17-35
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.
Application Deadline	3/31/2017 11:59:00 PM Eastern Time Zone
Description	**Research Topic Description, including Problem Statement**: Quantum secure communication (also called quantum key distribution) refers to the use of quantum effects to establish a communication channel secure against eavesdropping or tampering. Practical implementations of such channels have been developed for some time and technological solutions for free space channels are emerging. There are current initiatives in academia and industry to develop and deploy commercial Quantum Key Distribution (QKD) systems. The focus of current research and development is on implementation rather than embedding security principles at the design stage and this approach seems to be introducing a whole new set of potential avenues for attack that are not yet well understood. At this point in time there is little research into the vulnerabilities of practical implementations of QKD systems. CESG would like to encourage such research in order to build up a body of knowledge of how to attack and defend commercial QKD systems. We would also like to encourage more research into how to accurately assess the security of real-world devices that operate imperfectly and the development of methods for quantifying and validating the security claims of real-world QKD systems. Although QKD claims to provide guaranteed security, its responsible use must not introduce new vulnerabilities into real-world systems. This means that communication systems involving QKD should be designed with fail safe mechanisms that continue to operate securely even when the quantum part becomes compromised. **Example Approaches:** Example Approaches may include, but are not limited to:

Opportunity Title: Quantum secure communication
Opportunity Reference Code: IC-17-35

- Development of a mature body of practical QKD vulnerability research and accompanied by a development of methods for quantifying and validating the security claims of real-world QKD systems.
- Development of security methodologies for the design stage of QKD. A systematic taxonomy of attack vectors, costing of attacks of risk mitigation measures. One important and little-understood attack is denial-of-service.

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Business** (11 👁)
  - **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** (13 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)