

Opportunity Title: Emerging Technology Vulnerabilities

Opportunity Reference Code: IC-17-09

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-17-09

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

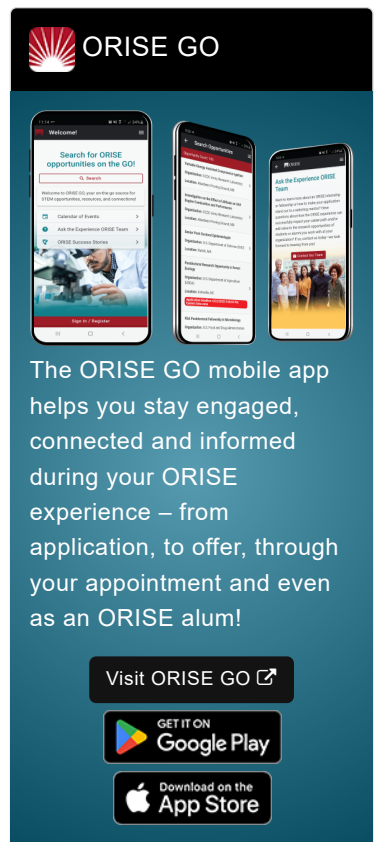
Description Research Topic Description, including Problem Statement:

Emerging technologies has been defined as those technical innovations which represent progressive developments within a field for competitive advantage.[1] In the last few years, the use of several emerging technologies has increased. Biometrics is used for access identification. Systems connected to the internet of things are increasing to include smart cities and smart grids. Screenless displays and mobile collaboration are beginning to replace traditional displays and video conferencing systems. Complex items can be produced through additive manufacturing. Unmanned vehicles are used in peacekeeping operations, fire-fighting, search and rescue operations, and surveillance. Documents and materials are being transferred, bought, and sold through services on the dark web. Cryptocurrencies can be used to digitally purchase items. Genetic engineering can be used to create ethnic bioweapons. A large number of these emerging technologies are potentially open to compromise or attack by outside entities. The goal of this effort is to determine if vulnerabilities exist, what they are, and how the technology user can guard against unknown vulnerabilities. Tools and techniques may also be developed to examine vulnerabilities.

Example Approaches:


A successful proposal could examine an emerging technology in order to answer at least one of the following questions:


- Determine vulnerabilities exposed by use of the technology.
- When using the technology, what steps should an individual take to guard against attack?
- What consequences could result if the technology is compromised, attacked, or leveraged for nefarious purposes, and how can it be mitigated?
- How can one emerging technology be used to protect security vulnerabilities in another emerging technology?


 OAK RIDGE INSTITUTE
FOR SCIENCE AND EDUCATION

ORISE GO

The ORISE GO mobile app helps you stay engaged, connected and informed during your ORISE experience – from application, to offer, through your appointment and even as an ORISE alum!

Visit ORISE GO 

GET IT ON
 Google Play

Download on the
 App Store

Opportunity Title: Emerging Technology Vulnerabilities

Opportunity Reference Code: IC-17-09

- 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](#))