Opportunity Title: Capability Limitations and Security of Cyber Biometric Authentication
Opportunity Reference Code: IC-16-41

Organization	Office of the Director of National Intelligence (ODNI)
Reference Code	IC-16-41
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	4/15/2016 6:00:00 PM Eastern Time Zone
Description	Organizations across the globe increasingly use biometrics to access information systems. In doing so, new databases are increasingly being developed to store and match the various biometric modalities (i.e. fingerprints, iris, voice, and facial recognition) that may be presented to various information systems. Although various vendor and academic studies have been conducted in response to the challenges presented by the use of biometrics in cyberspace, an authoritative study on this topic has not been conducted. This research is intended to reveal and explore the implications of using biometrics for authentication of information systems with a focus on the security issues associated with their use. Understanding these issues will provide a basis for improved analysis of existing and potential vulnerabilities. The proposed research will examine information system limitations and security issues related to individual or multiple biometric modalities used for authentication. **Example Approaches:** Projects for this topic could include: • The extent to which biometrics obtained involuntarily could be used for the authentication of information systems • The extent to which biometrics could be manipulated and introduced unknowingly into biometric databases • the extent to which repositories that store biometrics could be pilfered or tampered through cyber means • The extent to which biometrics used for authentication can be retrieved (remotely or manually) from mobile devices such as i-Phones, Android, or other similar information systems. • The scalability of how well biometrics contained in

Opportunity Title: Capability Limitations and Security of Cyber Biometric Authentication
Opportunity Reference Code: IC-16-41

information systems scale from a lab demonstration (with tens of users) to an enterprise-wide solution (with thousands of users). Scalability would address the impact on accuracy (false accept, false reject, and equal error rate), as well as in terms of the modality (e.g., fingerprints, iris, face, etc) and in terms of verification vs. identification

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 👁)