Opportunity Title: Risk-aware recommender systems for computer network defense
Opportunity Reference Code: IC-17-20

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-17-20

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**:

Computer network defense relies heavily on human operators and analysts but we have failed to monitor, analyze, optimize, or mitigate issues related to physical and cognitive limits that may threaten human and mission safety and productivity. This is a research project to study the potential for increased human resiliency using risk-aware recommender systems that leverage machine power to aid human computer defense activities.

Recommender systems have become increasingly commonplace in everyday life, from movie and music to online dating. These systems use past behavior and other data sources to help the user make more informed, relevant, and timely decisions. Despite large quantities of similar data, however, cyber security and computer network defense have underutilized historical data to inform human decisions.

Consider this example. An analyst in the security operations center is investigating suspicious web requests that may indicate an attack against his corporate webserver. The analyst suspects that blocking the machine generating the suspicious traffic may mitigate the problem. Should he take the action? A recommender system might recommend a different course of action based on historical knowledge about the webserver, suspected attacker, or even world events.

Recommender systems for cyber defense are likely to differ from existing solutions and approaches. Unlike stable and predictable recommender systems like Netflix, cyber defense is incredibly dynamic and must consider both historic and real-time information when recommending a course of action. Another difference is that Netflix is primarily concerned with optimizing the accuracy and relevance of its recommendations. Recommendations in cyber defense must be not only accurate and relevant, but must consider a variety of user-defined or machine-inferred risks of accepting (or rejecting) a recommendation.

Even if new technology can produce a recommender system for network defense, there may still be challenges related to human usability and

Opportunity Title: Risk-aware recommender systems for computer network defense
Opportunity Reference Code: IC-17-20

effectiveness. Research suggests that algorithm avoidance is a powerful detractor, and future work remains which considers human trust and acceptance of recommender systems in cyber security.

Unclassified Example Approaches:

Research proposals could describe innovative approaches to recommender systems that measurably improve human satisfaction, productivity, and/or operational security in computer network defense. Proposals may incorporate multidisciplinary approaches and consider:

- How can a recommender system improve computer network defense?
- What network defense data that is commonly collected today is valuable to the recommendation of future actions? What additional data, if collected, would measurably improve recommendations? How should that data be stored so that it can queried quickly, even as the volume and velocity of data increase?
- What new or existing algorithms can incorporate historical and real-time data to produce accurate and relevant recommendations? Under what conditions or situations does an algorithm produce accurate and trustworthy recommendations?
- Which methods and types of recommendation are most useful, compelling, and productive for human users? How do mental or behavioral limitations affect the utility and adoption of recommendation systems, and how can they be overcome?

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 👁)