Opportunity Title: Security for Internet of Things endpoints
Opportunity Reference Code: IC-17-37

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-17-37

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

The Internet of Things (IoT) is widely hailed as the next evolution of communication. The Internet of Things concerns the communication of billions of devices, to delivery an ever-increasing set of services to consumers, to businesses and to governments. To contrast, the Internet of People is limited in the region of seven billion, being the population of our planet. This is now approaching saturation, at least in the developed world. The Internet of Things has no such limits, and while projections vary, it is expected that there will be 20-40 billion connected devices at the start of the next decade.

Applications for IoT are still in their infancy, and generally centered on consumer or consumer-to-business use cases. Today we have personal health monitors, home management systems, smart meters and vehicle telematics as the most commonly used applications. Just around the corner are traffic management systems, buildings information management, environmental sensors, and in range are smart cities, industrial control systems and fully driverless cars.

The interconnectedness of all Things raises important questions about security and resilience. For example:

- How do we know if a device is working properly?
- Can we distinguish between failure due to error or due to malicious intervention?
- How do we protect the content and integrity of device communications?
- Do we even trust that a device really is what it claims to be?

There are also questions about the scope of trust. To what extent should trust functionality be global, mandated and subject to standardization? This would enable integration of systems, but potentially at the cost of agility and time-to-market.

Unclassified Example Approaches:

Opportunity Title: Security for Internet of Things endpoints
Opportunity Reference Code: IC-17-37

A common attribute of IoT endpoints is that they are small, low-power DC devices. This places constraints on hardware/software footprint to preserve form factor, and on power consumption to preserve battery life. With these constraints in mind, proposals could explore some of the following areas:

- Techniques which give assurance of a device's identity. The Internet today uses Public Key Infrastructures (mostly bases on X.509); the mobile/cellphone industry uses SIM technology. Compare these approaches for suitability in IoT devices and applications, to develop new techniques to optimize security within the constraints.
- To what extent can trust be delegated or federated? Again, Internet and mobile industries have solutions, such as login with Facebook, emerging FIDO standards, and inter-operator delegated authority in DECT, UMTS and LTE standards.
- Techniques for secure access to interfaces and services, both to and from endpoints. The Internet today has little in the way of standardization, using a mixture of cookies, URL-encoding and bespoke exchange of tokens. This is a particularly tough challenge for IoT given the range of applications. A precursor stage may be to develop an ontology for exchange of device-specific information models and interfaces.
- Cryptographic applications need keys, and key distribution is a huge and complex challenge. Public key cryptography attempts to solve this by reducing the complexity of key distribution, but it comes at high computational cost. In contrast, the mobile industry uses symmetric key distribution and key derivation in order to reduce connection times. For IoT we need better understanding of the driving characteristics in order to develop appropriate key management techniques.

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 👁)