Opportunity Title: International Technology Standards Setting: Cyber Security Opportunities Fellowship
Opportunity Reference Code: ICPD-2024-32

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-32

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 3 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.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

Description

Research Topic Description, including Problem Statement:

International technology standards development

International standards[1] are integral to the development, adoption and use of technology. They are a critical part of the global technology ecosystem as they help facilitate trade, provide first-movers with a strong competitive advantage, and can generate significant revenue for companies with large patent portfolios.

The international technical standards development landscape is primarily industry-led through multistakeholder standards development organizations (SDOs), where private sector and technical experts propose, debate, negotiate and approve the best technical standards to address common problems and interoperability.

Focusing on the technology environment, this project seeks to establish an accessible evidence base on the impact of technical standards on cyber security; the benefits of participating in SDOs; and factors affecting domestic experts' involvement in standards development.

Example Approaches:

Research proposals could approach this issue from a variety of disciplines, or as a cross-disciplinary effort. The research area touches on aspects of international relations; business;

telecommunications and critical technologies; information technology; internet engineering; and applied science. Proposals could consider some or all of:

- the impact of international standards on technology development
- the trends and challenges within the international standards-setting ecosystem.

Suggested approaches include:

- analysis of the role (historic and contemporary) of international telecommunications and cyber related SDOs
- analysis of the economic opportunities and risks of standards participation for industry—including opportunity cost and the impact of standards essential patents
- analysis of security implications of technology standards—including impact on and risks for cyber security; data security; and end-user privacy
- survey of the technology industry, academia and other expert attitudes on participation in relevant SDOs
- comparative review of international industry participation in cyber technology related SDOs
- case studies relating to Australian-developed technology standards or technology use cases.

Relevance to the Intelligence Community:

This project will help contextualize the role of international standards, inform government collaboration with business and academic partners, and support participation in the development of robust, secure standards for emerging and critical technologies.

As a key collaborator with business and academic partners on cyber and technology security, this project will support the NIC to better contextualize the role of international standards and support the development of robust, secure standards for emerging and critical technologies.

Reference:1 For the purpose of this project, international standards are considered to be documents developed through international SDOs that set out specifications, procedures and guidelines that aim to ensure products, services, and systems are safe, consistent, and reliable. This does not include normative guidance or advice.

Knut Blind, Martin Kenney, Aija Leiponen, Timothy Simcoe, (2023) ‘Standards and innovation: A review and introduction to the special issue’, Research Policy, Vol 52, Issue 8, https://doi.org/10.1016/j.respol.2023.104830.

Key Words: Standards Development Organizations (SDOs); Critical

Opportunity Title: International Technology Standards Setting: Cyber Security Opportunities Fellowship
Opportunity Reference Code: ICPD-2024-32

and emerging technologies; Internet Engineering Taskforce; International Telecommunications Union; Cyber Security Standard; Communication technology standards.

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (3 👁)
  - **Computer, Information, and Data Sciences** (17 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (30 👁)