



## **6<sup>th</sup> Annual Call for Proposals**

### **I3P Research Fellowships**

**for postdoctoral researchers, junior faculty and research scientists**

#### **Important Dates:**

**Applicants must submit proposals to host institutions by February 6, 2009**

**Host institutions must submit application packets to the I3P by February 20, 2009**

**Applicants will be notified by April 30, 2009**

#### ***Program Description***

The Institute for Information Infrastructure Protection (I3P) fellowship program is designed to build a nationwide cadre of investigators focused on critical infrastructure research challenges. The program also advances the I3P's national research agenda and provides expanded research opportunities at I3P consortium member institutions. A targeted goal of the I3P fellowship program is to add depth and breadth to critical research needs highlighted by the I3P [Cyber Security Research and Development Agenda](#) which identifies the following core research areas: Enterprise Security Management; Trust Among Distributed Autonomous Parties; Discovery and Analysis of Security Properties and Vulnerabilities; Secure System and Network Response and Recovery; Traceback, Identification, and Forensics; Wireless Security; Metrics and Models; and Law, Policy, and Economic Issues.

#### ***Eligibility***

Successful applicants will have received their Ph.D. no more than three years prior to **September 15, 2009**. Current students must complete all degree requirements prior to the commencement of the award. Fellowship candidates should have strong backgrounds in fields related to information infrastructure protection.

#### ***Award Information***

The I3P will appoint up to three fellows for one-year terms, pending the release of funding. Fellows must spend the term of their fellowship in residence at an I3P Consortium member

institution. Fellowship funding will be provided by the I3P and administered locally by the hosting institution. The I3P will provide up to \$150,000 per fellow to cover salary, fringe benefits, and travel, and to help offset the institutional costs associated with hosting a fellow. Moving expenses should be negotiated with the host institution. Joint appointments at two member institutions will be considered. A minimum stay of two months at the secondary institution is required. Fellows are expected to begin their fellowships between June and September. The host institution must agree to perform written mid-year and year-end reviews of a fellow's work and submit the reviews to the I3P administrative office. Fellows are expected to travel to at least one I3P Consortium meetings during the fellowship to present their research. Fellows should identify the I3P as the sponsor and the Department of Homeland Security as the funding source in all publications describing work done during the fellowship. In addition, fellows will be expected to comply with any guidelines imposed by their host institution regarding disclaimers on publications, and electronic copies of fellows' research publications must be submitted to the I3P administrative office three weeks prior to public release.

### *How to Apply*

#### **1. Applicant identifies and contacts a prospective host institution**

Each applicant must consult with an I3P Consortium member institution at which the applicant, if selected, would spend the term of his/her fellowship in residence. Applicants are encouraged to work with their prospective host institutions closely while developing their applications. Contact information for Consortium members participating in the fellowship program may be browsed on the [I3P Consortium Member Contacts page](#). Each applicant should submit the following:

- Cover letter; including citizenship and/or visa status
- Curriculum vitae; including a list of publications.
- Abstract and a three to five page description of the proposed research project: the description of research should address the relevance of the proposed work to areas identified in the I3P [Cyber Security Research and Development Agenda](#), anticipated outcomes of the work, the technical challenges and the approach.
- Three (3) letters of recommendation.

#### **2. Host institution completes and submits the application packet**

A complete application will include the candidate's cover letter, curriculum vitae, abstract and description of the proposed research project, letters of recommendation, and a letter from the host institution, including a preliminary budget. The host institution's letter should state that it agrees to host an I3P fellow, explain how the work will benefit the fellow; describe the research environment and equipment to which the fellow will have access; confirm the fellow's tasks and responsibilities; commit to provide the fellow with proper office and research space; and commit to submit two written reviews of the fellow's work. Host institutions must submit completed applications to the I3P in electronic form by **February 20, 2009** to Elisabeth.L.Bryan@Dartmouth.edu.

## ***The Selection Process***

Fellows will be selected based on the following criteria:

- Intellectual merit of the proposed work.
- Extent to which the proposed work suggests and explores creative and original concepts.
- Candidate's capabilities and plans to use metrics or measures of effectiveness for model.
- Clarity of the candidate's work plan, tasks, responsibilities, and deliverables.
- Feasibility, appropriateness, and potential impact on U.S. information infrastructure.
- Qualifications and research record of the applicant.
- Relevance of the proposed work to the I3P [Cyber Security Research and Development Agenda](#).
- Impact of recommendation letters from the host institution and external references.

Applications are reviewed thoroughly by the I3P fellowship committee, and each applicant is provided with a written review of his/her proposal.

## ***Contact Information***

All inquiries regarding a Consortium member institution's research interests or interest in hosting a candidate should be directed to the appropriate point of contact at each member institution. Contact information for Consortium members may be found at the I3P Consortium Members [I3P Consortium Member Contacts page](#).

***Participating Institutions:*** Purdue University ▪ University of Tulsa ▪ University of Idaho ▪ Columbia University ▪ University of California, Davis ▪ Cornell University ▪ George Mason University ▪ Georgia Institute of Technology ▪ Heinz School of Public Policy and Management, Carnegie Mellon University ▪ Idaho National Laboratory ▪ University of Illinois at Urbana Champaign ▪ New York University ▪ Dartmouth College ▪ Johns Hopkins University ▪ MIT Lincoln Laboratory ▪ The MITRE Corporation ▪ Pacific Northwest National Laboratory ▪ SRI International ▪ Indiana University ▪ The RAND Corporation ▪ University of Massachusetts Amherst ▪ University of Virginia.

### **Administrative or procedural questions should be directed to:**

Elisabeth Bryan  
I3P Program Assistant  
Elisabeth.Bryan@Dartmouth.edu  
(603) 646-0706

**This program is funded by the U.S. Department of Homeland Security.**