



8th Annual Call for Proposals

I3P Research Fellowships

for postdoctoral researchers, junior faculty and research scientists

Important Dates:

Applicants submit proposals to host institutions by February 4, 2011.

Host institutions submit application packets to the I3P by February 18, 2011.

Applicants will be notified by April 29, 2011.

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 such as those highlighted in the 2009 [National Cyber Security Research and Development Challenges](#). Some identified research areas include: Data Confidentiality, Integrity and Provenance; Metrics and Models; Human Behavior; and Law, Policy, and Economic Issues.

Eligibility

Successful applicants will have received their Ph.D. no more than three years prior to **September 15, 2011**. 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 two fellows for one-year terms, pending the release of funding. Fellows will spend the term of their fellowship in residence at an I3P Consortium member institution. Fellowship funding, 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, will be provided by the I3P and administered locally by the hosting institution. Moving expenses should be negotiated with the host institution. Joint appointments at two member institutions will be considered, where a minimum stay of two months at the secondary institution is required. Fellowships are expected to begin between June and September. The host institution will provide a written final review of a fellow's work to the I3P. Fellows are expected to travel to at least one I3P Consortium meeting to present their research. Fellows will 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 2009 [National Cyber Security Research and Development Challenges](#), 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 a written final review of the fellow's work. Host institutions must submit completed applications to the I3P in electronic form by **February 18, 2011**.

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 2009 [National Cyber Security Research and Development Challenges](#)
- 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](#).

Administrative or procedural questions should be directed to:

Heather Drinan
Associate Director of Research & Operations
Heather.Drinan@Dartmouth.edu
(603) 646-6472

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