

U. S. DEPARTMENT OF HOMELAND SECURITY

KENTUCKY CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Request for Research and Development Project Proposals

August 2007 Solicitation

**Issued By
The National Institute For Hometown Security
Somerset, KY**

The Kentucky Critical Infrastructure Protection (KCI) Program is carried out through the Kentucky Homeland Security University Consortium (Consortium) and managed by the National Institute for Hometown Security (NIHS). The program is focused on research, development and transfer to practical utilization of technologies designed to protect the nation's community based critical infrastructures. Research needs and requirements are determined by NIHS in consultation with the United States Department for Homeland Security (DHS). Funding for the program is provided by DHS.

In previous years the KCI has provided funding for twenty-three separate research and development projects. Each project requires that a Kentucky-based university serve as the lead institution for the research, development and coordination activities. Each project is also encouraged to have participation by at least one other Kentucky-based college or university and may also involve non-Kentucky universities and institutions. Private sector participation is also encouraged where appropriate.

The KCI experience with the existing twenty-three projects has led DHS to provide funding and support for a more advanced structure that is intended to allow for the production of more relevant and integrated technology solutions and to move the program toward national significance and long term stability. Universities and Principal Investigators who have participated in previous KCI projects will notice significant differences in the current solicitation and subsequent project management process.

Summary of Program Requirements and Changes:

1. As in previous years, the KCI program strongly encourages all proposals to involve at least two member institutions of the Consortium. This approach is intended to promote collaboration and to build homeland security expertise and capacity within the Consortium. Projects may include more than two Consortium members and may also include non-Kentucky universities, other research institutions and private sector partners. A Consortium member institution must serve as the overall project lead.
2. In the interest of avoiding any action that might discourage a project proposal, no set limit has been placed on the size, cost or duration of a project. A review of KCI project history would indicate that the majority of projects are funded for less than \$1 million, many for much less, and none has a life exceeding three years.
3. Although DHS will continue to make final project selection decisions, contracts for those projects selected for award will be issued and managed by NIHS. Contracts will be

between NIHS and the lead Consortium member identified in the project proposal. The lead university will be responsible for issuance and management of any sub-agreements necessary to complete the project.

4. NIHS will make payments to universities receiving project awards based on milestones agreed upon at the time of award. Payments will not be made on a time and materials or cost reimbursement basis. NIHS will retain the ability to withhold payments and to cancel contracts to assure compliance with contract terms, project reporting requirements, and performance against established milestones. Project budgets and schedules should be planned accordingly.
5. In addition to the cost of executing the proposed project, budgets should account for travel and related expenses for participation by the project PI and other relevant project personnel in mandatory Project and Program Review Conferences. These conferences will occur in April and November of each year and take place in the Washington, D.C. area. Budgets should also account for travel to Somerset, Kentucky, in February and July of each year for required program and project status meetings.
6. In managing and overseeing projects selected for award, NIHS intends to make heavy use of internet and web based tools. This will include utilization of a secure internet site to promote communication and for posting information and reports in their required forms
7. DHS has recognized the value of the KCI program and its emphasis on commercialization and conversion to use of new technologies. DHS provided NIHS with a funding mechanism that allows for a unique intellectual property ownership and management arrangement. This arrangement will be reflected in the contract agreement between NIHS and those lead universities receiving project awards. The proposed arrangement will allow NIHS to assume the lead role in commercializing the new technologies and to share in any resulting license or royalty stream, but will neither interfere with existing university intellectual property policies nor diminish any financial interest that the research team may otherwise have in the project.
8. Projects will be evaluated and selected by DHS against the following criteria. Offerors are encouraged to consider these criteria in preparing proposals.
 - **Technical Merit:** Projects will be reviewed by a DHS assembled panel of subject matter experts. The team will evaluate the proposed research in terms of its uniqueness, its ability to substantially improve infrastructure protection, its potential for achieving national impact, and its relationship to existing technology and other similar research efforts which may be underway.
 - **Technical Feasibility:** The DHS panel of experts will provide an assessment of the overall feasibility of achieving the goals of the project within the time and budget proposed. Included in this evaluation will be the depth and range of the present state of the technology being proposed, as well as the capabilities of the proposed development team and facilities. Formation of cross-university teams is strongly encouraged as a way to enhance the technical feasibility of the effort.
 - **Relevance and Integration:** Each proposal will be required to identify which of the NIHS technical topic area or areas the project is designed to address. The DHS selection team will evaluate, from a systems perspective, how effectively the proposed research or product could be utilized in addressing a specific CIP problem or issue. Proposals demonstrating a

systems understanding of CIP issues and providing a clear concept of operations or description of how the product would be used will be favored. In addition, a business case should be presented that identifies potential customers for the work, an estimate of the size of the market that would be served, competing technologies or research activities, potential for commercialization, and an estimate of final cost of the product, if applicable.

- **Commercialization/Conversion to Use Plan:** All projects should be designed and planned to ease conversion of the resulting technology, information or product to the marketplace or other practical use. Proposals will be evaluated on the level of thought, pre-planning, and steps taken to demonstrate a path and likelihood of successful commercialization or utilization of the project result in support of community based critical infrastructure protection.
- **Project Management and Execution Plan:** Consideration will be given to university and PI experience in managing and executing other similar research and development projects. This will extend to arrangements between the lead university and other project partners. The establishment of a realistic plan of execution at a reasonable total cost will influence selection decisions.

CALL for PROPOSALS:

White Papers:

NIHS has designed a two tier process for its 2007 project solicitation cycle. Beginning September 10, 2007, 2007 NIHS will accept white paper summaries of proposals for new, community based critical infrastructure protection research projects. These white papers are intended to provide a summary and overview of the proposed project. All white papers must be submitted on the template available for download from the NIHS website at www.thenihs.org. Included within this white paper template are instructions for completion, as well as a listing of the technical topic areas of interest to NIHS and DHS in this project solicitation. For convenience these topic areas are attached to this Request for Proposals and are also available on the NIHS website. In submitting a project for consideration the offeror should clearly identify which of these topic areas the proposal is intended to address. Completed white papers should be returned electronically by following the instructions for secure uploading available at the NIHS website. Only electronic versions of the white papers will be accepted. The website will be activated on September 10, 2007. The deadline for submission of white papers is 5:30 PM EDT on September 14, 2007, after which they will no longer be accepted by the NIHS website.

Full Proposals:

Following a preliminary review by NIHS, all qualifying white papers will be forwarded to DHS for detailed review. DHS will review the white papers and select proposals for whose offerors will be encouraged to submit full proposals. NIHS anticipates transmitting these encouragements for full proposals by mid-November 2007. Additional information on requirements for those projects encouraged to submit full proposals will be provided at a later time. These requirements will include utilization of a submission template similar to that used in the white paper process, as well as attendance and participation at a daylong training session to be held in Somerset, Kentucky, designed to support and enhance the offerors' ability to

meet DHS and NIHS needs and requirements. The date for this training session will be announced simultaneously with the encouragements for full proposals. Those offerors not encouraged to submit_ full proposals will be notified of this decision as well.

Project Solicitation Conference:

Offerors are very strongly encouraged to familiarize themselves with all program requirements prior to submission of white papers and proposals. NIHS will host a **Project Solicitation Conference** to present these requirements, including all proposed contractual obligations on **Tuesday August 14 at the Center for Rural Development in Somerset, Kentucky**. In addition to discussion of program requirements, the Solicitation Conference will provide insight into the technical topic areas and may be helpful to offerors in enhancing understanding of project selection criteria, the conference will begin at 10:00 AM and extend through 3:30 PM (EDT). A full conference agenda is available at the NIHS website and those interested in attending are asked to register at via the website at www.thenihs.org. The registration form will be available on the website after July 10, 2007. There is no charge for attendance at the Solicitation Conference.

NIHS will also host a conference call from 10:00 AM through 11:00 AM (EDT) on Tuesday August 21 to respond to questions related to the project solicitation process, program requirements or other management matters. A summary transcript of the conference call will be provided to all those registering for the Solicitation Conference and will be posted on the NIHS website as soon as practical following the call. Details of the conference call access will be provided at a later date.

NIHS reserves the right to amend this process at any time.

Technical Needs & Requirements

Research and Development Themes

The Kentucky Critical Infrastructure (KCI) Program is carried out through the Kentucky Homeland Security University Consortium and managed by the National Institute for Hometown Security (NIHS). From its inception, this program has been focused on the research and development required to provide the tools and technologies needed to address Community Based Critical Infrastructure Protection needs.

As the program moves into the next, more advanced phase, NIHS and DHS have developed an integrating framework for the program around the topic of resiliency. We define resiliency as the ability to detect, avoid, deter, protect against, respond to, and recover from infrastructure disruptions. DHS and NIHS will use this framework to direct the program toward efforts that will improve the resiliency of communities, groups of communities, and regions in dealing with infrastructure disruptions.

As part of our program improvement strategy with DHS, we will be requesting that the responders to this solicitation present a business case for their projects. This involves a statement of the problem to be solved, its importance to hometown security from a systems perspective, an identification of potential customers for the solution, an estimate of cost and market size for any developed products, and discussions of competing technologies. The responders may want to initiate discussions with other entities, e.g., business schools, within the Kentucky university system for help in meeting this requirement. Alternatively, outside entities, e.g., the Council on Competitiveness in Washington, DC, has expressed interest in providing support.

The research agenda supporting this new direction includes the following topics:

I. Detection

- A. Develop tools to detect and mitigate animal and crop disease outbreaks. Tools should be scalable for use by small farmers. Suggest countermeasures.
- B. Develop new, less expensive, interoperable sensors to guide and protect first responders when entering an unsafe area. This could include sensors that report structural conditions, stability of damaged infrastructure, or presence of hazardous gases.
- C. Develop advanced surveillance and detection methods for intruders/malicious activities in cluttered urban areas. Examples include wide area surveillance at airports and underwater monitoring. This could include real-time verification of individual identities using multiple biometric methods.
- D. Develop inexpensive methods for detecting waterborne or underwater threats approaching waterfront facilities (ports, dams, locks, ports, refineries, LNG/LPG etc.)
- E. Develop non-destructive methods to assess conditions of critical infrastructures, for example, geophysical methods used in a tunnel to determine the material properties of the surrounding soils as well as properties and integrity of the tunnel.
- F. Provide systems engineering concepts and schema for linking interoperable sensors together to improve detection probabilities.

II. Prevention

- A. Provide methods and models for conducting risk assessments that can be used by communities, groups of communities and regions. This activity should use modeling and simulation tools to analyze vulnerabilities and consequences and to map interdependencies. The interest is in identifying critical nodes at the state and local level, attaining a better understanding of cascading impacts caused by a disruption within defined areas of interest, and developing mitigation plans to minimize the impacts of such events. Use of case studies is encouraged. This activity should, as appropriate, build on, and coordinate with, existing work by DHS, specifically, the National Infrastructure Simulation and Analysis Center (NISAC) and the Center of Excellence for Risk and Economics at the University of Southern California.

- B. Simplify and validate models for vulnerability assessments of selected critical infrastructures to blast and projectiles, including underlying mechanics.
- C. Identify and/or develop physical testing methods and capabilities for blast model validation, including underwater blasting and centrifuge testing.
- D. On a regional basis, analyze the risk associated with disruption of key nodes, including communications capabilities, that could impact the resiliency of the national transportation infrastructure.

III. Protection, Response, and Recovery

- A. Develop concepts, principles, and approaches for restarting infrastructure services in a community that has experienced a wide-spread disruptive event.
- B. Develop rapid automated response and fast recovery technologies to minimize disruption of critical infrastructure services.
- C. Explore the concept of self-healing infrastructures for one of DHS's defined infrastructure sectors. The energy infrastructure is excluded.
- D. Develop improved systems for communications across multiple jurisdictions, including multi-band radio capabilities with a goal of achieving interoperability among first responder agencies and other Federal agencies.
- E. Develop methods for interdicting waterborne or underwater threats approaching waterfront facilities (ports, dams, locks, ports, refineries, LNG/LPG etc.).
- F. Develop concepts for creating facilities that are inherently resilient by using careful site selection, blast resistant materials, etc.
- G. Design and develop protective measures for selected critical infrastructure against blast and projectiles. Identify and test advanced materials for protection against blast and projectiles.
- H. Design or develop effective, low cost protective measures for commercial and government facilities. Include schools/campuses. Develop concepts for how these measures could be used to provide intrinsic (built-in) security.

I. Develop concepts and preliminary designs for adaptable, low cost replacements for critical infrastructure components that have long replacement times, e.g., bridges, dams, locks. These replacements could be temporary or permanent depending on the need.

J. Develop special, rapidly deployable, low cost structural support that can be engineered into a facility or deployed by first responders to prevent catastrophic structural failure.

IV. Preparedness

A. Identify and/or develop tools that may assist communities in their efforts to build resiliency on a community, state and regional basis.

B. Using modeling and simulation tools and other analytical approaches where appropriate, evaluate plans and tools in the areas listed below. Conducting gap analyses, identify weaknesses, and develop improved plans and/or tools to address the gaps.

1. Risk assessment methods for food and agriculture sectors. Tools must be capable of addressing risk in these disaggregated and diverse sectors.

2. Tools that may assist communities in their efforts to build resiliency on a community, state and regional basis. Include analysis of economic viability.

3. Technologies or best practices that can minimize the impact or mitigate the effects of a cascading failure. This will involve understanding dependencies and interdependencies. It will also be necessary to investigate human relationship issues, such as forming partnerships and developing trust.

4. Existing continuity of business and continuity of operations plans and/or tools for communities and among communities.

5. Models that capture best practices for acquisition of needed technology and for planning and operational responses to disruptive events. Identify those that could be further modified to evaluate potential new solutions.

6. Information technology tools that can assist communities in obtaining information in a timely fashion to monitor critical infrastructures and respond to disruptive events.

7. Modeling and simulation capabilities that evaluate the efficacy of, and recommend improvements to, existing community plans for dealing with serious disasters or business continuity, including the ability to test multi-jurisdictional coordination.

8. Surge capacity and scalable evacuation models that include interdependencies among communities on a state or regional basis. This will require awareness of, and coordination with, FEMA's community evacuation model development.

9. Best practices and tools for sheltering a large number of people, to include associated logistical support that addresses needs of special populations, e.g., elderly. Best practices that foster a culture of self-sufficiency for residents, businesses, and communities without federal assistance for the first two weeks after a serious event. Emphasize community interdependencies and/or specific, large facilities or events involving large numbers of people.

C. Design and populate a system to identify and quickly communicate situational awareness among supply chain providers of essential services or commodities in communities and/or regions.

D. Develop a community operational plan for dealing with pandemics. Identify how and who enforces a shelter-in-place policy. Identify what infrastructure needs to be added to provide for mitigation. Identify how communities prepare and train to operate under severe and long term shelter- in-place requirements. Address impacts of pandemics on schools. Working with public health preparedness agencies, identify and improve existing plans for dealing with the surge in demand for hospitals. Identify and improve plans to ensure that power and water/wastewater and trash collection services continue uninterrupted during this time span. Provide a plan for utilizing help from volunteers during the emergency. Translate findings from a national plan (DHS/NISAC) into use by local, state, and regional planners.

E. Develop and implement a program for raising the awareness and engagement of high school students in homeland security issues and problem solutions.

V. Other

A. Address other analysis or tool development needs for improving the resiliency of regional or national critical infrastructures.

B. Working with DHS/NISAC, develop seminars for discussing community responses to pandemics and identify needs and requirements of state and local responders.

++++