National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge

Overview

When a solution to a capability or technological gap is identified within the critical infrastructure community, it is often difficult for certain projects and ideas to receive the funding or buy-in to fully develop and implement the idea or project. Using a partnership-building approach through the NIPP Security and Resilience Challenge, the Office of Infrastructure Protection (IP)—within the Department of Homeland Security's National Protection and Programs Directorate—in partnership with the National Institute of Hometown Security (NIHS), provides an opportunity for the critical infrastructure community to help identify, develop, and fund state-of-the-art, cost-effective technology, tools, processes, and methods that address near-term needs and strengthen the security and resilience of critical infrastructure.

The Challenge is unique in that it helps identify and fund innovative ideas that can provide technologies and tools to the critical infrastructure community that are ready or nearly ready to use. However, projects funded under the NIPP Challenge are meant to not only have tangible, near-term results so they can be quickly developed and implemented, but also be financially, practically, and logistically sustainable in the long term so that they can enhance the security and resilience of critical infrastructure across multiple sectors for years to come. These ideas, due to their innovation and research, can be risky, but are likely to offer important benefits to the critical infrastructure community.

To learn more about the 2017 NIPP Security and Resilience Challenge, please visit www.thenihs.org.

Funding Structure

The Challenge leverages an "Other Transaction Agreement (OTA)" through the National Institute of Hometown Security (NIHS) to allocate funding for a projected 6-12 projects in Fiscal Year (FY) 2017. Submissions undergo a capability gap identification process directed at solving specific problems. By encouraging cost-sharing agreements, the Challenge can yield benefits for all stakeholders.

Areas of Interest

- Ideas leading to results with demonstrated impact on critical infrastructure security and resilience in the next 2-3 years
- Needs and requirements that have been previously identified, but not yet funded
- Existing or past solutions that require upgrading or help in transitioning-to-use
- Novel ideas with high potential to enhance critical infrastructure security and resilience, particularly those involving partnerships
- Ideas from sectors and regions that are "shovel ready" and can be quickly implemented
- Ideas that can scale across the critical infrastructure community and different sectors

Evaluation Criteria

NIPP Challenge submissions are evaluated by an NIHS independent panel, according to IP criteria:

Qualifying Criteria

- Does the proposed submission provide a new and innovative solution to the identified gap/problem or address new or emerging risks?
- Does the proposed submission fall within IP's mission scope?
- Does the proposed submission classify as research?

Alignment and Partnership

- To what extent does the proposed submission align to the Joint National Priorities for Critical Infrastructure Security and Resilience and/or NIPP Calls to Action (see www.dhs.gov/nipp)?
- To what extent are there identified resource-sharing (e.g., in-kind, cost, personnel) agreements to support the submission?
- To what extent does the proposed submission integrate physical-cyber, cross-sector, or other types of integration/dependencies?
- To what extent does the proposed submission integrate cross-sector partnerships or expand into new stakeholder groups?

Viability and Impact

- To what extent is there a feasible path for the proposed submission to be transitioned-to-use for the critical infrastructure community?
- What is the anticipated scale of impact of the proposed submission in increasing the security and resilience of U.S. infrastructure in the next 2-3 years?
- To what extent can the proposed submission be financially, practically, and logistically sustained to create longer-term impacts on critical infrastructure security and resilience?
- To what extent can the proposed submission be accomplished with Challenge funding? (I.e., Can funds from the Challenge result in substantial progress?)

Contact Information

NIPP Security and Resilience Challenge Program Manager
Jay Robinson
Senior Policy Analyst
DHS, Office of Infrastructure Protection
703-235-9581 (Office)
202-740-8728 (Mobile)
jay.robinson@hq.dhs.gov

NIPP Security and Resilience Challenge Subject Matter Expert
John Taylor
Chief Technical Officer
National Institute for Hometown Security
606-451-3450 (Office)

NIHS Project Leader
Amanda White
Project Manager
National Institute for Hometown Security
606-451-3452 (Office)
606-425-2655 (Mobile)
awhite@thenihs.org

***

The NIPP Security and Resilience Challenge is managed by the Office of Infrastructure Protection, within the National Protection and Programs Directorate of the Department of Homeland Security (DHS), in partnership with the National Institute for Hometown Security.