DHS Science and Technology Directorate

National Critical Infrastructure Security and Resilience Research and Development Plan

Purpose and Background

The purpose of the National Critical Infrastructure Security and Resilience (CISR) Research and Development (R&D) Plan is to identify National R&D Priority Areas that inform R&D investments, promote innovation, and guide research activities across the critical infrastructure community. The Plan should inform current and future R&D direction in support of CISR and complement public and private R&D activities and programs in these areas.

In February 2013, President Obama issued Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, and Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, underscoring the Administration's commitment to strengthening the security and resilience of critical infrastructure.

PPD-21 directed the Department of Homeland Security (DHS), in coordination with the Office of Science and Technology Policy, Sector-Specific Agencies, the Department of Commerce, and other Federal departments and agencies, to develop a National CISR R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The Science and Technology Directorate (S&T) was designated lead responsibility for facilitating development of the Plan.

As its title suggests, the National CISR R&D Plan is a national plan, not a Federal Government or a DHS plan. The audience includes the critical infrastructure community and others with an interest in advancing CISR R&D.

The National CISR R&D Plan was developed through a collaborative process involving public and private stakeholders from across the critical infrastructure community. DHS conducted outreach through various mechanisms to seek input to the Plan.

National R&D Priority Areas

The National R&D Priority Areas represent the core of the National CISR R&D Plan. They reflect feedback and ideas from a range of partners and stakeholders engaged throughout the Plan's development.

The National CISR R&D Priority Areas are as follows:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk assessment and management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action;
- Build a crosscutting culture of CISR R&D collaboration.

Plan Implementation

Effective implementation of the National CISR R&D Plan will require collaboration across the critical infrastructure community. Stakeholders should work collectively to define R&D requirements and design and implement solutions that meet identified needs.

The Federal CISR R&D community will convene a subcommittee under the National Science and Technology Council to align Federal and federally funded R&D activities that seek to strengthen CISR. After the subcommittee is formed, S&T will begin development of an Implementation Strategy, with input from interagency stakeholders, outlining Federal steps to implement the Plan and identifying key deliverables for aligning Federal R&D activities. The Implementation Strategy also will describe how S&T will coordinate with CISR stakeholders to develop annual performance metrics by National R&D Priority Area, to track the alignment of CISR R&D activities.

The National CISR R&D Plan encourages all stakeholders to develop and share reliable measures to evaluate the effectiveness of R&D activities in strengthening CISR. The Plan also informs sector-level R&D planning, which should include the evaluation of sector contributions to advancing the National R&D Priority Areas.

Homeland Security
Science and Technology

To learn more about the National CISR R&D Plan, contact S&T at CISR-R&D@hq.dhs.gov.

May 2015