IMPLEMENTATION ROADMAP FOR THE NATIONAL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE RESEARCH AND DEVELOPMENT PLAN

PRODUCT OF THE

Critical Infrastructure Security and Resilience Subcommittee

Committee on Homeland and National Security

OF THE NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

December 2016

EXECUTIVE OFFICE OF THE PRESIDENT
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
WASHINGTON, D.C. 20502

December 15, 2016

Dear Colleagues,

Strengthening the resilience and security of the Nation's critical infrastructure is an ongoing priority for the Federal government. Sixteen critical infrastructure sectors support the Nation's economy, society, and national security. It is essential that these sectors be protected against all threats and hazards so that the services they provide continue during disruptive events.

As critical infrastructure systems become increasingly interdependent, ensuring their security and resilience becomes more complex. Targeted research and development efforts are needed to anticipate new threats and hazards to infrastructure systems and mitigate potential cascading effects across sectors. Federal departments and agencies are key stakeholders in critical infrastructure and are uniquely positioned to initiate much of this research and development.

I am pleased to release the *Critical Infrastructure Security and Resilience (CISR) Research and Development (R&D) Implementation Roadmap,* which outlines Federal R&D priorities and activities to strengthen critical infrastructure security and resilience. The Implementation Roadmap was ordered by the *National CISR R&D Plan* (December 2015) and developed by Federal departments and agencies via the National Science and Technology Council, with input from external stakeholders. The contents of the Implementation Roadmap reflect the Federal Government's continuing commitment to support critical infrastructure.

Sincerely,

Steve Fetter
Principal Assistant Director
National Security and International Affairs
Office of Science and Technology Policy

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development (R&D) enterprise. One of the NSTC's primary objectives is establishing clear national goals for Federal science and technology investments. The NSTC prepares R&D packages aimed at accomplishing multiple national goals. The NSTC's work is organized under five committees: Environment, Natural Resources, and Sustainability; Homeland and National Security; Science, Technology, Engineering, and Mathematics (STEM) Education; Science; and Technology. Each of these committees oversees subcommittees and working groups that are focused on different aspects of science and technology. More information is available at www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976. OSTP's responsibilities include advising the President in policy formulation and budget development on questions in which science and technology are important elements; articulating the President's science and technology policy and programs; and fostering strong partnerships among Federal, state, and local governments, and the scientific communities in industry and academia. The Director of OSTP also serves as Assistant to the President for Science and Technology and manages the NSTC. More information is available at www.whitehouse.gov/ostp.

About the Critical Infrastructure Security and Resilience Subcommittee

The Critical Infrastructure Security and Resilience (CISR) Subcommittee is an interagency group chartered under the NSTC Committee on Homeland and National Security. It was convened in December 2015 in response to Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and the *National CISR R&D Plan* to develop an implementation roadmap for R&D activities to improve the security and resilience of critical infrastructure and to help coordinate Federal CISR R&D efforts.

About this Document

This document was developed by the CISR Subcommittee. The document was published by OSTP.

Acknowledgements

The CISR Subcommittee acknowledges the contributions from CISR working groups, previous Subcommittee co-chairs from OSTP and DOE, DHS National Protection and Programs Directorate staff, and the IDA Science and Technology Policy Institute for providing subject-matter expertise, constructive review, and other contributions to the development of this document.

Printed in the United States of America, 2016.

Report prepared by

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
COMMITTEE ON HOMELAND AND NATIONAL SECURITY
SUBCOMMITTEE ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

National Science and Technology Council

Chair
John P. Holdren
Assistant to the President for Science and Technology and Director,
Office of Science and Technology Policy

Staff
Afua Bruce
Executive Director

Committee on Homeland and National Security

Chairs
Steve Fetter
Principal Assistant Director for National Security & International Affairs
Office of Science and Technology Policy

Reginald Brothers
Under Secretary for Science and Technology
Department of Homeland Security

Stephen Welby
Assistant Secretary of Defense for Research & Engineering
Department of Defense

Staff
Tod Companion
Executive Secretary
Department of Homeland Securit

Critical Infrastructure Security and Resilience Subcommittee

Co-Chairs

Department of Homeland Security
Department of Energy
Office of Science and Technology Policy

Subcommittee Members and Contributing Departments and Agencies

Departments
Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of State
Department of Transportation
Department of the Treasury

Agencies
Defense Advanced Research Projects Agency
Environmental Protection Agency
Federal Aviation Administration
Federal Communications Commission
Federal Emergency Management Agency
Federal Energy Regulatory Commission
Federal Highway Administration
Food and Drug Administration
General Services Administration
National Institute of Standards and Technology
National Science Foundation
Nuclear Regulatory Commission
United States Army Corps of Engineers
United States Bureau of Reclamation

Executive Office of the President
National Security Council
Office of Management and Budget
Office of Science and Technology Policy

Table of Contents

Executive Summary

Critical infrastructure provides essential services to the Nation and requires proactive and coordinated efforts to ensure that it is secure and able to withstand and rapidly recover from all hazards. Hazards include threats and incidents of natural disasters, cyber-attacks, industrial accidents, pandemics, terrorism, sabotage, and destructive criminal activity that targets critical infrastructure. These hazards warrant action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. Research and development (R&D) is needed to understand the behavior of infrastructure systems in the face of threats and vulnerabilities, increase system resilience, and improve risk management.

Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience* (February 2013) describes the importance of improving the security and resilience of the Nation's critical infrastructure to natural disasters and terrorist attacks, and the *National Critical Infrastructure Security and Resilience Research and Development Plan* (November 2015) identifies five National Priority Areas for R&D investment. This Implementation Roadmap builds on these documents by outlining Federal R&D activities in support of the identified National Priority Areas.

Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*

PPD-21 was issued on February 12, 2013 and establishes a national policy on critical infrastructure security and resilience and identifies the role of the Federal Government in that effort.

"The Federal Government…has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators."

The policy identifies strategic imperatives for a Federal approach to meet this responsibility, including an effort to align those Federal and federally-funded R&D activities that "seek to strengthen the security and resilience of the Nation's critical infrastructure."

The Implementation Roadmap identifies R&D priorities and presents concrete activities Executive departments and agencies to conduct over the short term (1–3 years), medium term (3–10 years), and long term (10 years or more). Each of the activities is organized by five Challenge Areas, including:

1. **Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making**: Leverage data-rich repositories, quantitative models, and visualizations to improve overall risk management and resource allocation processes for the Nation's critical infrastructures; thereby enhancing the resilience and security of interdependent infrastructures

2. **Position, Navigation, and Timing (PNT) Support Functions**: Enhance the security and resilience of critical PNT-dependent systems through the development of robust PNT services and equipment that ensure the continuity and integrity of vital services

3. **Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems**: Create safe, secure, and resilient municipal water infrastructure systems by developing new technologies and integrating them into existing systems

4. **Next-Generation Building Materials and Applications for Transportation Infrastructure Systems**: Build a resilient, sustainable, adaptable, and durable smart transportation infrastructure that incorporates high-performing materials, optimized structural designs, advanced sensor systems, and fabrication and construction processes that meet mobility and livability challenges
5. **Resilient and Secure Energy Delivery Systems**: Develop technologies, models, and analytic tools that enable energy owners and operators to design, implement, operate, and maintain secure and resilient energy delivery systems that are capable of sustaining critical functions during and after disruptive events

By specifying activities that will lead to improvements in the five Challenge Areas and identifying the agencies responsible for them, this Implementation Roadmap will help ensure that the Federal Government and its critical infrastructure partners are able to withstand, prepare, and adapt to changing conditions and rapidly recover from the effects of extreme hazard events.

Introduction

In February 2013, President Obama issued Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, to strengthen the security and resilience of the Nation's critical infrastructure against both physical and cyber threats.[1] PPD-21[2] outlined the importance of strengthening and maintaining the Nation's critical infrastructure so that it is able to withstand and rapidly recover from all hazards.[3] PPD-21 emphasizes that the ability to identify, assess, and mitigate threats and hazards to critical infrastructure is essential and that "proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems—that are vital to public confidence and the Nation's safety, prosperity, and well-being." Understanding, quantifying, and predicting the behavior of infrastructure systems in the face of threats and vulnerabilities is critical for risk management and is made possible through critical infrastructure security and resilience (CISR) R&D efforts. R&D efforts are needed to ensure infrastructure services continue uninterrupted under both normal operating conditions and infrequent, but high-impact, events.

This document (referred to as the "Implementation Roadmap" or "Roadmap") identifies key areas in which R&D is needed to advance the security and resilience of physical infrastructure and outlines "proactive and coordinated efforts" between Federal agencies that

Case Study: Project Jack Rabbit

Project Jack Rabbit is an example from the chemical sector that demonstrates the importance of R&D to improve the security and resilience of critical infrastructure. In 2005, a freight train collision in South Carolina released 60 tons of chlorine gas, causing over 250 people to seek treatment for chlorine exposure and resulting in $30–$40 million in disaster-related costs. Following the disaster, Congress expressed concern that railcars carrying chlorine and other toxic inhalation hazard (TIH) chemicals put the public at risk for similar chemical releases caused by accidents or acts of terrorism. The Department of Homeland Security (DHS) Transportation Security Administration and Science & Technology Directorate cosponsored the DHS Chemical Security Analysis Center to develop the critical data necessary to improve models of potential TIH releases from accidents or terrorist attacks on chemical storage tanks and railcars. In 2010, chemical and railroad sectors updated safety protocols and mitigation strategies based on results from Project Jack Rabbit.

---

1 Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, governs the Federal Government's response to any cyber incident, both government and private.

2 Presidential Policy Directive 21 (PPD-21). *Critical Infrastructure Security and Resilience*. February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

3 According to PPD-21:

> "Resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
>
> "Secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.
>
> "All hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

will advance the state of CISR.[4]

PPD-21 directs the Secretary of DHS, in coordination with the Office of Science and Technology Policy (OSTP), the critical infrastructure Sector Specific Agencies (SSAs),[5] and other Federal departments and agencies to align those Federal and federally-funded R&D activities "that seek to strengthen the security and resilience of the Nation's critical infrastructure."[6] To meet this directive the *National Critical Infrastructure Security and Resilience Research and Development Plan* ("the Plan") was provided to the President in November 2015.[7] PPD-21 requires that the Plan "take into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments."

National Priority Areas

The Plan builds on past and ongoing CISR R&D activities across the 16 critical infrastructure sectors. The Plan also identifies five National Priority Areas that are intended to inform R&D investment and guide research throughout the critical infrastructure community. The National CISR R&D Priority Areas are:

A. Develop the foundational understanding of critical infrastructure systems and systems dynamics;

B. Develop integrated and scalable risk assessment and management approaches;

C. Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;

D. Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and

E. Build a crosscutting culture of CISR R&D collaboration.

The audience for the Plan includes critical infrastructure owners and operators and other stakeholders with an interest in advancing future R&D for the security and resilience of the Nation's critical infrastructure. The Plan represents a coordinated and collaborative approach to reduce critical infrastructure risk and enhance resilience to threats and hazards. The National CISR R&D Priority Areas are intended to serve as a set of broad, overarching categories that will improve the security and resilience

---

[4] Research and development as defined by Office of Management and Budget (OMB) Circular No. A–11 (2015), page 8 of Section 84.

[5] PPD-21 identifies 16 critical infrastructure sectors and designates associated Federal SSAs: DHS for Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Emergency Services, Information Technology, and Nuclear Reactors, Materials, and Waste; Department of Defense (DOD) for Defense Industrial Base; Energy: Department of Energy (DOE) for Energy; Department of the Treasury (DOT) for Financial Services; United States Department of Agriculture (USDA) and Department of Health and Human Services (HHS) for Food and Agriculture; DHS and General Services Administration (GSA) for Government Facilities; HHS for Healthcare and Public Health; DOT and DHS for Transportation Systems; and Environmental Protection Agency (EPA) for Water and Wastewater Systems.

[6] Any incident that may possibly be a terrorist incident (I.e., not clearly caused by natural events) will be treated as an actual terrorist incident, until determined otherwise, by the Attorney General.

[7] *National Critical Infrastructure Security and Resilience Research and Development Plan*, November 2015, https://www.dhs.gov/publication/national-critical-infrastructure-security-and-resilience-research-and-development-plan.

of critical lifeline functions[8] or address threats and hazards that are crosscutting, affecting multiple sectors, and leading to broad regional or national-level consequences.[9]

The Plan identifies several categories of activities within each of the National Priority Areas, including, but not limited to, characterizing infrastructure systems to build an integrated understanding; developing technology solutions that can secure and enhance the resilience of cyber and physical systems; analyzing policies and regulations that might enable and incentivize CISR enhancements; and applying social and behavioral sciences to model and identify ways to manage the human role in CISR. The Plan calls on critical infrastructure stakeholders to leverage existing collaboration structures, develop new working relationships, and enhance data sharing and communication to implement R&D efforts.

To implement the Plan and facilitate Federal interagency coordination, the CISR Subcommittee was convened under the National Science and Technology Council (NSTC). The CISR Subcommittee has identified critical infrastructure subject matter experts and thought leaders with national perspectives to develop an Implementation Roadmap that identifies CISR R&D priorities, presents concrete activities for Executive departments and agencies (agencies), and provides awareness to the critical infrastructure community.

Implementation Roadmap Challenge Areas

To help scope the Implementation Roadmap and identify distinct short term (1–3 years), medium term (3–10 years), and long term (10 years or more) R&D activities, the CISR Subcommittee identified a set of Challenge Areas through a review of relevant critical infrastructure sector R&D strategy documents, input from Federal subject matter experts, and feedback from the Critical Infrastructure Partnership Advisory Council (CIPAC).[10] The technical advances that apply to the cyber-dependent aspects of critical infrastructure and address the most pressing CISR cyber R&D needs identified in the Plan are described in *The Federal Cybersecurity Research and Development Strategic Plan* (February 2016) and are not addressed in this document.[11] The Challenge Areas focus on three of the four lifeline functions and are consistent with the five National Priority Areas for CISR R&D identified in the Plan. Communications is the lifeline function not currently addressed in the Implementation Roadmap due to the substantial private sector investment in R&D associated with the sector. The five Challenge Areas are:

1. Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making
2. Position, Navigation, and Timing Support Functions
3. Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems
4. Next-Generation Building Materials and Applications for Transportation Infrastructure Systems
5. Resilient and Secure Energy Delivery Systems

---

8 Lifeline functions include communications, energy, transportation, and water (DHS, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, December 2013, 16).

9 The U.S. coasts support highly concentrated populations and resources; impacts to these areas can easily disrupt multiple sectors, leading to the disruption of critical social, economic, and natural systems throughout the country (Beck 2014).

10 CIPAC facilitates interaction between representatives from the government and those from the community of critical infrastructure owners and operators for the purposes of deliberating and forming consensus positions to assist the Federal Government.

11 Areas not explicitly covered in *The Federal Cybersecurity Research and Development Strategic Plan* are addressed through specific activities in the Implementation Roadmap.

The Implementation Roadmap is organized around these Challenge Areas and describes goals for ongoing Federal and non-Federal CISR R&D associated with the Challenge Area. The Challenge Area goals map to the National Priority Areas for CISR R&D identified by the Plan (Table 1).

Table 1. CISR R&D Challenge Area Goals Mapped to National CISR R&D Priority Areas

Goal	Associated Priority Areas from CISR R&D National Plan (listed on p. 3)
Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making	
Models of Critical Infrastructure Interdependencies on Lifeline Functions	A, C, D
Data to Support Predictive Models and Decision Making	C, D, E
Effective and Efficient Decision Processes for Resource Allocation	C
Position, Navigation, and Timing Support Functions	
Technologies to Harden PNT Receivers	A, C
Technologies to Enable More Secure and Resilient PNT Services	A, C
Technologies to Enhance the Security of Current and Future PNT Systems	C
Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems	
Resilient Water and Wastewater Infrastructure	A, C
Methods and Strategies for Response to Disasters	B, C, D
Smart Water Systems for Water Resilience and Security	C
Next-Generation Building Materials and Applications for Transportation Infrastructure Systems	
Modernized Critical Transportation Infrastructure	C
Transportation Infrastructure to Withstand Extreme Events	C
More Rapid, Efficient and Cost-Effective Building and Repair of Transportation Infrastructure	A, C
Diagnostic Capabilities for Assessing the Performance and Condition of Infrastructure	C
Resilient and Secure Energy Delivery Systems	
System Design for Resilience	C, D
Preparedness and Mitigation Measures	B, C, E
Energy System Response and Recovery	C, E
Characterization and Management of Energy Interdependencies	B, C, E
Energy Systems that Withstand High-Impact, Low-Frequency Events	B, C
Develop Next-Generation Cybersecurity Capabilities	C

Priority activities to achieve the goals of each Challenge Area were identified by the CISR Subcommittee and by working groups of Federal subject matter experts. Each activity has an identified lead agency, expected output, and expected timeline for completion (i.e., short term, medium term, and long term). Each activity in this Roadmap should be consistent with existing agency authorities. The Roadmap also discusses the role of non-Federal stakeholders in CISR R&D activities.[12]

How DHS Will Develop Annual Performance Metrics

The Plan states that DHS will coordinate with CISR R&D stakeholders to develop annual performance

[12] This information is derived from subject matter expertise, engagement with stakeholders, and interviews.

metrics by National CISR R&D Priority Area, to provide a means of tracking the alignment of R&D activities that strengthen CISR. The last section of the Roadmap describes next steps for engagement with critical infrastructure owners, operators, and stakeholders. DHS will coordinate with CISR R&D stakeholders to develop metrics that measure R&D activities and to what extent they are strengthening CISR. DHS will work through existing coordination mechanisms, such as the Sector Coordinating Councils (SCCs) and SSAs, to collect the data that will be used to inform the metrics, and to demonstrate progress across Roadmap activities. This can be accomplished through direct coordination with the identified lead agencies to track and measure performance. The first annual metrics will be developed within six months of issuance of this Roadmap. The Roadmap will align to and inform other current reporting efforts, such as the National Critical Infrastructure Assessment Report[13] and the National Preparedness Report[14] to ensure continued support of other national efforts to enhance security and resilience. The CISR Subcommittee will review, update, and issue the National CISR R&D Plan every four years, with interim updates as needed. Future updates to the Roadmap will be coordinated with the updates to the Plan.

Note: The actions specified in the National CISR R&D Implementation Roadmap are intended to inform the policy development process and are not intended as a budget document. The commitment of Federal resources to support these activities will be determined through the annual budget process.

[13] The annual National Critical Infrastructure Assessment Report measures the effectiveness and progress of critical infrastructure protection and resilience efforts by Federal, State, local, tribal, and territorial governments and the sectors through a set of outcome statements and associated metrics.

[14] The National Preparedness Report is an annual requirement of PPD-8, *National Preparedness*.

Challenge Area 1: Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making

Vision Statement

Leverage data-rich repositories, quantitative models, and visualizations to support improved overall risk management and resource allocation processes for the Nation's critical infrastructures, thereby enhancing the resilience and security of interdependent infrastructures.

Introduction

Increased connectivity across critical infrastructure sectors has led to interdependencies that create both vulnerabilities and opportunities that cannot be addressed exclusively within the policy frameworks of individual infrastructure sectors. When infrastructure performance and recovery for hazards are modeled and planned for in isolation, corresponding approaches to mitigation and response may not adequately account for cascading and interdependent effects that cut across multiple sectors, with potentially devastating emergent effects.[15] Understanding, quantifying, and predicting the behavior of interdependent infrastructure systems in the face of threats, vulnerabilities, and opportunities require not only further research, but also testing and development of practical tools that are user friendly.

Current understanding of the design and operation of infrastructure systems is insufficient to support detailed modeling and prediction of the effects of interdependencies on the services provided by these systems. Available data on operations and consequences are scattered, not standardized, and are often not in the public domain, severely limiting opportunities for developing, validating, and calibrating models of infrastructure systems. Additional work in this area has the potential to contribute to ensuring continued provision of infrastructure service both under normal and extraordinary conditions and during disruptive events (such as large-scale disasters).

Successful management of infrastructure interdependencies and design requires close cooperation and collaboration among owners, operators, and Federal agencies supported by robust tools, data, and input from customers. Available tools to support these activities are not uniformly mature and are of limited use for making decisions on investments that bear directly upon interdependencies. Research focused on the development and use of data, methods, models, and tools for understanding interdependencies can improve decision making at all levels of society, reduce threats, and enhance performance in interdependent infrastructures.

Recent research, motivated in large part by historical experiences of societal response to disruptive events, has adopted an integrated view of technological and human elements in interdependent infrastructure systems. This view is reflected in the recognition that people play an important role in the design, operation, and renewal of infrastructure systems and that the need for newer technologies to support changing societal demands for infrastructure services is ongoing. On the near horizon is ever-tighter coupling between human and technological components in infrastructure. This section identifies key R&D goals and activities across sectors to enhance understanding of interdependency effects on lifeline functions, particularly in relation to improved decision-making processes and resource allocation.

[15] *Emergent* effects are phenomena that are not readily predictable from an understanding of individual elements of a system.

Goals

The following three goals for Challenge Area 1 support increasing the resilience and security of interdependent infrastructures:

1.1 Models of critical infrastructure interdependencies on lifeline functions

1.2 Data to support predictive models and decision making

1.3 Effective and efficient decision processes for resource allocation

Achieving these goals will require characterization and analysis not only of physical and cyber interdependencies among infrastructure sectors, but also of the social, organizational, regulatory, political, and economic factors that help determine the flow of vital services these sectors provide.

1.1. Models of Critical Infrastructure Interdependencies on Lifeline Functions

Considerable R&D has been conducted to develop theoretical models of interdependent infrastructures, yet comprehensive and data-based studies of human and technological aspects of infrastructure design and performance are rare. Case studies of past natural disasters and terrorist attacks suggest the importance of existing and emergent features of infrastructure systems. Improved quantitative modeling of physical infrastructure systems and associated human behavior is needed to capitalize on lessons of the past.

1.1.1. Through an interagency process, identify and characterize lifeline function interactions among sectors. Characterization will include identification of key physical, social, and behavioral effects on critical infrastructures to enable model development. Stakeholder agencies for this objective include the National Institute of Standards and Technology (NIST), DHS, National Science Foundation (NSF), and other relevant agencies.

Deliverables: (1) Requirements for the selection and integration of data and metadata into models of infrastructure interdependence; (2) a taxonomy of social and behavioral influences on mitigation, response, and recovery processes; and (3) a crosswalk of sector interdependencies at the community, industry, regional, and national levels to identify key physical, operational, economic, social, and behavioral relationships necessary to support model development.

Timeline: Short term

1.1.2. Link existing models of the effects of interdependencies across critical infrastructure sectors on system service, security, and resilience. DHS will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) Formats for data exchange that facilitate data use across different infrastructure models; (2) federated models that combine existing analytical tools at various levels of granularity; and (3) a gap analysis of existing data and models.

Timeline: Short term

1.1.3. Develop models that predict physical interdependencies for all hazards. DHS will coordinate this activity with other relevant agencies. This activity will depend, in part, on the interdependency mapping produced by Activity 1.1.1 and the data sets developed under Goal 1.2.

Deliverables: (1) Predictive models of positive and negative cascading effects and feedback loops in vulnerabilities, resilience, and recovery of critical infrastructure systems; and (2) mathematical models and computational algorithms that better capture critical physical dynamics of interdependent infrastructures at multiple spatial and temporal scales.

Timeline: Short to medium term

1.1.4. Support research and development on predictive models of human behavioral responses to all hazards to inform critical infrastructure design and operations. NSF, NIST, and other relevant agencies will support and coordinate this activity, which will depend, in part, on the interdependency mapping produced by Activity 1.1.1 and the data sets developed under Goal 1.2.

Deliverables: (1) Predictive models of human behavioral response to various hazards at multiple scales (e.g., individual, community, and population) in interdependent infrastructure systems; and (2) mathematical and computational models that better capture utilization patterns of critical infrastructure services at multiple scales.

Timeline: Medium term

1.1.5. Create models that predict both designed and emergent interdependencies for all hazards, including their physical and behavioral effects. The United States Army Corps of Engineers (USACE) and other relevant agencies will coordinate this activity, which will depend, in part, on the physical and behavioral models produced by Activities 1.1.3 and 1.1.4.

Deliverables: (1) Predictive models of critical infrastructure response to all hazards, accounting for causes and effects of both physical and human behavioral aspects; (2) computational models of cascading effects and interdependencies in critical infrastructure systems, and their role in vulnerability, resilience, and recovery assessment; and (3) models that forecast the influence of human behavior on infrastructure dynamics over multiple spatial and temporal scales.

Timeline: Long term

1.1.6. Collect and analyze data to model the effects of aging and degradation on infrastructure systems over typical planning periods of 10 to 100 years, including the role of maintenance. Granting agencies with expertise in materials and structural systems will coordinate this activity.

Deliverable: Predictive models for infrastructure systems and mathematical descriptions of aging and degradation processes and interactions, including how system performance depends on maintenance, repair, and retrofit practices.

Timeline: Medium term

1.2. Data to Support Predictive Models and Decision Making

Federal, State, and local governments and infrastructure owners and operators have collected substantial amounts of data on human and mechanical systems and processes in interdependent infrastructures. These data exist in various locations and in multiple formats that lack standard measures, definitions, and taxonomies. Moreover, while there is an active research community in this area, comprehensive standardized data sets are lacking. Work is therefore needed to explore and address issues of data availability, verification, normalization and integration to support data use within and across communities and regions. These data must also be made available to the appropriate research communities, whether through secure portals, non-sensitive synthetic data derived from the raw data, or other means. To support predictive modeling efforts (and thus planning and policy decisions), gaps in existing data (and data collection protocols) must be identified and addressed.

In addition to data describing the physical configuration and performance of infrastructure systems, predictive modeling of infrastructure security and resilience will also rely on social science data sets describing human behavior during and after disruptive events.

1.2.1. Collect and curate existing data for standardization and validation of predictive models relating to infrastructure interdependencies across critical infrastructure SSAs and stakeholders. DHS, NSF, NIST, and other relevant agencies will promote and coordinate.

Deliverables: (1) Data sets in the public domain to support model development, identification of issues of timing, standardization and validation of data collection efforts, and solutions to issues of data storage and dissemination; and (2) develop data repositories to support efforts in data distribution and in the development and validation of critical infrastructure models.

Timeline: Short term

1.2.2. Support research and development on tools and techniques for creating synthetic data suitable for critical infrastructure modeling. NSF and other relevant agencies will promote and coordinate this activity.

Deliverable: Synthetic data sets at the community, regional, and industry levels that can be used by researchers, model developers, and planners without handling concerns necessary for proprietary or other restricted-distribution data.

Timeline: Short term

1.2.3. Collect, generate, validate, and publish existing, new, and synthetic data on critical infrastructure design and performance. NIST, in consultation with DHS, will collaborate with other agencies to coordinate, sponsor, and promulgate guidance on this activity.

Deliverables: (1) Criteria for normalizing data on infrastructure design and performance from diverse sources; (2) taxonomies for data on infrastructure design and operations, including economic data and data characterizing infrastructure interdependencies; and (3) data repositories to support public and private efforts to develop and validate models of the behavior of interdependent infrastructure systems.

Timeline: Short term

Deliverable: Data collection guidance for Federal, State, local, tribal, and territorial governments and infrastructure owners and operators, including the frequency, format, prioritization, and distribution of data on interdependent critical infrastructures.

Timeline: Medium term

1.3. Effective and Efficient Decision Processes for Resource Allocation

Research in the management of critical infrastructure, including interdependencies, is just beginning to explore the continuum from adaptive design, mitigation, and short-term response to after-event mitigation and longer-term recovery processes. To quantify tradeoffs between rapid recovery to a prior state versus longer-term activities following disasters, further work is needed to inform resource allocation decisions on how best to undertake post-event activities. The ongoing evolution of infrastructure technologies, the populations they serve, and the regulatory environment in which infrastructures operate further complicates R&D in this area. For example, restoration of electric power following the attacks of September 11, 2001, provided an unexpected opportunity to implement longer-term plans for the redesign of New York's electric power distribution network, but the implementation had to be balanced against the urgent, shorter-term need to secure reliable power for customers in the days and weeks following the attacks.

1.3.1. Develop models and tools for locating, deploying, and managing mitigation and response resources for interdependent infrastructure sectors. DHS will coordinate with SSAs on this activity.

Deliverable: Decision technologies, data analytic tools, and information visualizations to support the location and deployment of response resources for emergencies and disasters in interdependent critical infrastructures.

Timeline: Medium term

1.3.2. Develop models of how the sequence of decisions affects outcomes from response through recovery operations. DHS, NIST, and other relevant agencies will coordinate this activity.

Deliverables: (1) Characterization of sequential dependencies and tradeoffs in response and recovery alternatives; and (2) models of sequential dependencies and attendant tradeoffs during response and recovery of services provided by interdependent infrastructures, to include factors such as cost and substitutability of the resources used to create or convey such services for improved decision making.

Timeline: Medium term

1.3.3. Identify how evolving demand for infrastructure services, together with new technologies, can be analyzed to inform the design of new and more resilient interdependent critical infrastructure systems. NIST, DHS, and other relevant agencies will coordinate this research.

Deliverables: (1) Characterization of the changing demand for infrastructure services over the next 20 years for an appropriate set of communities; (2) emerging technologies that could either drive or respond to changing demand for infrastructure services; and (3) tools and techniques for analyzing how new technologies may affect the resiliency and sustainability of interdependent infrastructure systems.

Timeline: Medium term

Challenge Area 2: Position, Navigation, and Timing Support Functions

Vision Statement

Enhance the security and resilience of critical PNT-dependent systems through the development of robust PNT services and equipment that ensure the continuity and integrity of vital services.

Introduction

PNT equipment, including Global Positioning System (GPS) and other Global Navigation Satellite System (GNSS) technologies, is becoming more prevalent in the everyday lives of American citizens. Many of the Nation's critical infrastructure sectors have come to rely on GPS and other PNT technology to conduct their core missions. Examples include the use of precise PNT information to support timing synchronization for communications and power systems, highly accurate and reliable position services for emergency responders and agriculture, and navigation services for trucks, railways, and aircraft. For certain sectors, gaps in the receipt of critical PNT information or incorrect PNT information could result in unacceptable disruption of critical public services. Understanding how to reduce vulnerabilities and create a more robust, resilient, and secure set of integrated PNT services will protect the Nation's critical infrastructure from the consequences of PNT service disruptions caused by intentional or unintentional interference and other hazards.

Goals

The following three top-level goals for Challenge Area 2 seek to create a more robust and secure set of PNT services:

2.1. Technologies to harden PNT receivers

2.2. Technologies to enable more secure and resilient PNT services

2.3. Technologies to enhance the security of current and future PNT systems

These goals will help mitigate and prevent myriad consequences that could result from PNT disruptions, as more private sector and critical infrastructure sectors rely increasingly on PNT services to conduct core missions.

2.1. Technologies to Harden PNT Receivers

Develop technologies to harden PNT receivers (existing and future) to improve the ability to mitigate interference and spoofing threats at the PNT equipment subsystem level allowing for greater robustness. This includes the use of multi-GNSS and independent PNT sources to determine, in real time, the health or confidence of PNT information to the user applications.

2.1.1. Understand existing and emerging threats to receivers and chipsets from interference, spoofing, jamming, and cyber-attacks, to reduce and possibly eliminate these vulnerabilities, and to improve the integrity, availability, and continuity of PNT receiver components and PNT equipment. DHS, Department of Defense (DOD),[16] and Department of Transportation (DOT) will work with other

[16] The DoD is coordinating closely with DHS and DOT on the issues and goals addressed in this section. Subject to limitations and prohibitions associated with sharing classified national security information and technology solutions regarding these dual-use PNT technologies with private, non-government organizations, the DoD will provide inputs as required.

agencies and the private sector (particularly the manufacturing and user communities), as appropriate, to coordinate this activity. The Federal Communications Commission (FCC) shall be invited to participate.[17]

Deliverable: A report of findings to increase manufacturer and user community awareness of critical PNT-dependent user application system vulnerabilities to improve the resiliency of technologies used within critical application systems.

Timeline: Short term

2.1.2. Advance PNT receiver and other PNT technologies to be used in and interoperable with new and legacy PNT subsystems. Examples of potential R&D activities may include improved integration of GPS and multi-GNSS with terrestrial radio frequency and autonomous sensors; improved logic and algorithms for receiver components, software assurance, and cyber protections; and improved antenna hardware and processing (e.g., nulling antenna). DHS, DOD, and DOT will work with other agencies and the private sector (particularly the GPS and GNSS manufacturing communities), as appropriate, to coordinate R&D activities.

Deliverable: Pilot-ready prototype PNT receivers and PNT systems that incorporate new advanced elements that will improve the identification and mitigation of existing and anticipated future interference, spoofing, and cyber threats to the extent practical to enable the provision of PNT services to critical user application systems.

Timeline: Short to medium term

2.1.3. Improve next-generation PNT equipment so that it can use sources of PNT information in addition to GPS, possibly including independent and external PNT sources, such as broadcast signals, or internal PNT sources, such as inertial measurement units and chip-scale atomic clocks. DHS will work with DOT, DOD other agencies, and the private sector, as appropriate, to coordinate this activity.

Deliverable: Adaptable, pilot-ready prototype PNT equipment and systems that incorporate at least one additional independent PNT information source, if possible, to enable improved integrity cross-checks, more informed PNT decision making, and greater redundancy and consistency of PNT information integration into PNT-dependent critical applications.

Timeline: Medium term

2.2. Technologies to Enable More Secure and Resilient PNT Services

Identifying, researching, and developing technologies to enable more secure and resilient sources of PNT information can create more robust PNT services resistant to disruption and resilient to signal losses in any single service.

2.2.1. Identify and describe PNT R&D and technology needs and applications for critical infrastructure sectors. DHS would support the identification of timing needs, while DOT will support the identification of positioning and navigation needs. NIST, in collaboration with DHS, DOT, DOD, and the private sector, as appropriate, will map the national timing infrastructure.

Deliverable: (1) PNT technology needs for all sectors of critical infrastructure; and (2) an architectural map of the Nation's national timing infrastructure that identifies the interconnections

[17] To the extent the FCC is referenced in 2.1.1 and subsequent sections within this document, the FCC will participate to the extent it determines such participation is consistent with its statutory authority and legal obligations.

and interdependencies of clock networks to include the DOT Wide Area Augmentation System, the DOD master and alternate clocks, NIST time scales, and similar navigation aids.

Timeline: Short term

2.2.2. Develop a curated repository on Federal efforts to address GPS-related issues that can inform R&D efforts to produce new secure and resilient PNT services and technologies. DOT, in coordination with DHS and in consultation with DOD, will conduct this activity.

Deliverables: A curated repository that captures (1) efforts of the synchrophasor community within the Department of Energy (DOE) and DHS, (2) advances in intelligent transportation systems and future PNT needs for autonomous vehicles by DOT, and (3) research on aviation navigation and positioning systems (including aircraft and ground infrastructure systems) conducted by DOT.

Timeline: Short term

2.2.3. Conduct research, development, testing, and evaluation on the results of non-GNSS PNT technologies to meet PNT needs for critical infrastructure. DHS will complete this activity in coordination with DOD and other stakeholders. FCC shall be invited to participate.

Deliverable: Periodic reporting on the findings of non-GNSS timing technologies to improve understanding and inform R&D efforts to enhance existing PNT systems and services for critical infrastructure.

Timeline: Short to long term

2.2.4. Produce new assured PNT concepts for a robust, redundant, and self-healing network of primary PNT sources. DHS and DOT will coordinate this activity.

Deliverable: Peer-reviewed scientific papers on new assured PNT concepts

Timeline: Medium term to long term

2.3. Technologies to Enhance the Security of Current and Future PNT Systems

Enhancing the next generation of civil GPS signals and improving interference detection and mitigation (IDM) approaches for PNT services can increase the robustness and resilience of PNT systems and services. Activities for IDM can support R&D efforts to establish a nationwide ability to identify, detect, locate, auto-report, and mitigate GPS disruptions (e.g., interference, jamming, and spoofing). These improvements would enhance the ability of users to share information with stakeholders and enable enforcement actions when appropriate.

2.3.1. Identify gaps in current modernization plans for civil GPS signals to determine what added security measures, such as data authentication, may be integrated into future GPS signals. DHS and DOT, in coordination with DOD, will complete this activity.

Deliverable: A report on how to address identified gaps in modernized civil GPS signals.

Timeline: Short term

2.3.2. Identify Federal and civil IDM needs. DHS and DOT will coordinate this activity in consultation with DOD. FCC shall be invited to participate.

Deliverable: Federal and civil IDM science and technology needs

Timeline: Short to medium term

2.3.3. Share PNT disruption reports, where appropriate, to inform the R&D community as appropriate. DHS, DOT, and DOD will coordinate this activity. FCC shall be invited to participate.

Deliverable: Disruption reports

Timeline: Medium term

2.3.4. Develop and mature the technologies for IDM that are compatible with next generation PNT equipment. DHS, DOT, and DOD will coordinate this activity. FCC shall be invited to participate.

Deliverable: Technologies for improved decision making.

Timeline: Medium term to long term

Challenge Area 3: Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems

Vision Statement

Create safe, secure, and resilient municipal water infrastructure systems by developing new technologies and integrating them into existing systems.

Introduction

From the customer's viewpoint, technologies that provide uninterrupted water services that meet all applicable regulatory and quality standards not only protect public health but ensure safe, secure, and resilient municipal water systems. R&D is needed to create innovative, scientifically validated, cost-effective tools (including models); to develop methodologies to assess, diagnose, improve, repair, or upgrade aging infrastructure systems; and to ensure uninterrupted water services. There is also a need to operate water services in a more cost-effective and environmentally sound manner. R&D to meet these needs includes developing data-driven techniques and approaches that respond to events in real time.

As the water and wastewater sector strives to further advance capabilities and prepare for incidents that threaten public health, it needs innovative solutions to maintain effective and resilient operations. Lessons learned from post-incident analysis can provide a unique opportunity to identify critical needs that can be applied to improve responses to future incidents. Mechanisms are needed to make information available within and across critical infrastructure sectors to inform response and recovery decisions.

In the long term, the ability to maintain safe and sustainable water resources for humans and the environment through the development of next-generation technology, engineering, and processes will make water and wastewater systems more secure and resilient.[18] An area of focus to achieve this goal is the development and demonstration of individual technologies and integrated systems to improve the collection, treatment, and distribution of drinking water and wastewater and the recovery of water resources.

Goals

The following three goals for Challenge Area 3 support increasing the resilience and security of water and wastewater infrastructure:

- 3.1. Resilient water and wastewater infrastructure
- 3.2. Methods and strategies for response to disasters
- 3.3. Smart water systems for water resilience and security

These three goals will lead to a more secure and resilient water and wastewater system by addressing the most pressing current, future, and event-specific gaps in R&D.

---

[18] EPA, *Safe and Sustainable Water Resources: Research Action Plan 2016–2019*, https://www.epa.gov/sites/production/files/2015-10/documents/strap_2016_sswr_508.pdf.

3.1. Resilient Water and Wastewater Infrastructure

A modern secure and resilient water and wastewater infrastructure that meets the needs of consumers and creates a sustainable water system from source to tap to disposal. This includes systems that optimize water use and reuse and next-generation materials that are compatible with legacy systems.

3.1.1. Develop system-wide approaches for assessment of transformative fit-for-purpose and resource-recovery-based water systems. The Environmental Protection Agency (EPA) plans to coordinate this activity.

Deliverable: An open source database (e.g., a toolkit library) that contains a repository of detailed water-related technical options and perspective papers to serve water professionals and decision makers looking for specific transformative solutions that have been evaluated and assessed.

Timeline: Short term

3.1.2. Provide a system-level assessment of alternative fit-for-purpose water reuse scenarios for urban environments. This involves an integrated assessment approach combining life-cycle costing, life cycle impact assessment, local human health risks, and resilience capable of evaluating the role of scale, type of wastewater, and treatment approach on the sustainability of alternative scenarios. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) A new life-cycle assessment tool and database that will be able to quantify location-specific environmental impacts (such as eutrophication and water scarcity) for community water systems; and (2) a novel approach through coupling the system water scarcity with a total water assessment model to assess sustainable solutions for water shortages.

Timeline: Short term

3.1.3. Enhance water supply sustainability through an improved understanding and reduction of adverse environmental impacts associated with advanced water treatment processes. The Department of the Interior (DOI) will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Published results and progress in the United States Bureau of Reclamation Annual Report on improved seawater intakes and outfalls, concentrate management, energy efficiency, and renewable energy incorporation.

Timeline: Long term

3.1.4. Characterize brackish groundwater resources and assess environmental impacts of inland brackish groundwater desalination. DOI will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: An update to the United States Geological Survey brackish groundwater resources and an assessment of inland brackish groundwater technologies and associated environmental impacts to identify research gaps in this area.

Timeline: Long term

3.1.5. Evaluate emerging energy neutral or energy positive treatment technologies for resource recovery and energy conservation through Net Zero project research. EPA and USACE will coordinate this activity.

Deliverable: A published report on the evaluation of an emerging energy neutral or energy positive treatment technology (e.g., Anaerobic Membrane Bioreactor) for water reuse and resource recovery through a joint 2013 funding solicitation from EPA's Office of Research and Development and DOD's environmental technology demonstration and validation program.

Timeline: Short term

3.1.6. Develop innovations for water systems, including treatment technologies and methods for evaluating nontraditional disinfectants. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables:
Treatment technologies—(1) Innovative treatment technologies developed through EPA's Water Technology Innovation Cluster, which focuses on performance, public acceptance, regulatory and policy drivers or barriers, and business and economic development potential of innovative technologies; and (2) reports and case studies on existing EPA projects targeting the development, transfer, and adoption of near-commercially ready technologies that address agency priorities.

Nontraditional disinfectants—(1) A systematic process for acquiring the necessary data to create contact time (CT) tables for inactivation of pathogens (existing and emerging) using new or existing disinfectants (initially a "design of experiment" effort to establish an experimental matrix that can provide the data and analysis necessary to create CT tables); and (2) standard operating procedures and frameworks for testing and evaluating disinfectants.

Timeline: Short term

3.1.7 Research small distribution systems and premise plumbing to ensure safe water in small systems and buildings. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) An assessment of water conservation impacts on water quality in distribution systems, including recommendations on "right-sizing" plumbing for distribution systems through EPA's National Center for Environmental Research grant program; (2) published reports on water quality changes in premise plumbing and distribution systems due to lower flows; and (3) small-scale models to predict water quality in homes, buildings, and consecutive water systems (e.g., hospitals).

Timeline: Long term

3.2. Methods and Strategies for Response to Disasters

Proven strategies and methods for detection, mitigation, exposure assessment, and treatment of water system contamination as well as characterization and decontamination of water infrastructure (drinking water and wastewater systems).

3.2.1. Develop water system modeling tools that enable utilities to have situational awareness of the operations within their water systems (e.g., minute-to-minute conditions). EPA and USACE will coordinate this activity.

Deliverables: (1) A suite of hydraulic and water quality modeling tools that provide information to help detect a contamination incident, backtrack to identify the location, and optimize mitigation of the response for quicker return to service; and (2) periodically published EPA reports and open-source code computer models to help utilities and commercial entities use software as part of their modeling efforts for daily operations.

Timeline: Short to long term

3.2.2. Test and evaluate commercial off-the-shelf (COTS) detection and mitigation technologies and methods for contaminations in water systems. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) Data on performance of COTS online monitors for biological, chemical, and radiological contamination that will enable utilities to detect water quality or flow incidents and respond quickly to mitigate any public health or operation all threats; and (2) periodically published EPA reports and professional literature and information for inclusion in recommendations developed by EPA.

Timeline: Long term

3.2.3. Evaluate and modify existing human exposure models for water-related exposures. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) Models of water systems that fill gaps in the understanding of potential human exposure pathways from a water or wastewater system and conceptual exposure models that connect environmental concentrations and exposure pathways to potential exposures in wastewater systems; and (2) periodically published EPA reports, professional literature, and information for inclusion in recommendations developed by EPA.

Timeline: Long term

3.2.4. Develop innovative sample strategy options, sample collection methods, and analytical protocols for chemical, biological, and radiological contamination of water and wastewater systems. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) Sample collection and processing of complex water matrices and priority biological, chemical, radiological contaminants, and toxins; and (2) updated and new methods for relevant contaminants and matrices in the Selected Analytical Methods for Environmental Remediation and Recovery.

Timeline: Long term

3.2.5. Assess methodologies and strategies for water infrastructure decontamination and water treatment. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: (1) Contaminant-specific pilot to bench to field-scale research and testing for decontamination of water infrastructure; and (2) periodically published EPA reports and professional literature and information for inclusion in recommendations developed by EPA.

Timeline: Long term

3.2.6. Research rapid response and collect related data for information sharing to inform mitigation and recovery efforts. NSF will support this activity for RAPID awards.

Deliverables: (1) All publications resulting from a RAPID[19] award adhere to new requirements to improve information sharing and ensure long-term data preservation. These new requirements will include depositing publications within 12 months of initial publication to the NSF Public Access Repository, providing a minimum set of machine-readable metadata elements in a metadata record free of charge upon initial publication, and a reminder to ensure long-term preservation; and (2) rapid

[19] The RAPID funding mechanism is used for proposals having a severe urgency with regard to availability of, or access to data, facilities or specialized equipment, including quick-response research on natural or anthropogenic disasters and similar unanticipated events.

research response plan developed through the Standing Committee on Medical and Public Health Research During Large-Scale Emergency Events. The development of this plan will include discussions on how to disseminate data collected from research beyond publication and other research efforts, how to store the data, and outcomes for future use during other disaster responses.

Timeline: Short to long term

3.3. Smart Water Systems for Water Resilience and Security

Smart water systems that allow utilities to have situational awareness through the integration of hydraulic and water quality models and real-time data from sensors in the water system (supervisory control and data acquisition data). After assessing these conditions, this smart system can also automatically respond to incidents (e.g., those related water quality and contamination or cyber disruptions). Related R&D will lead to proven strategies and methods for detection, mitigation, exposure assessment, and treatment of water system contamination as well as characterization and decontamination of water infrastructure (drinking and wastewater systems).

3.3.1. Develop and disseminate measurement tools and NIST-traceable standards to enable the accurate identification and characterization of hazards and contaminants and allow for consistent performance measurement of systems across municipalities. NIST and USACE will coordinate this activity.

Deliverable: Methods and NIST-traceable traceable standards to support the water-sector monitoring and detection technologies for response to disasters.

Timeline: Long term

3.3.2. Develop the requirements for and assess the feasibility of a national test-bed network to support the development of innovative methods and technologies for energy-positive water resource recovery. NSF, DOE, EPA, and the Department of Agriculture (USDA) will support or coordinate this activity with private sector engagement, as appropriate.

Deliverables: Two workshops that produce related reports to describe the requirements and feasibility of a national test-bed network for wastewater treatment method and technology development.

Timeline: Short term

3.3.3. Derive approaches for optimizing EPANET[20] software for modeling small distribution systems and premise plumbing. EPA will coordinate this activity with other departments and agencies, as appropriate.

Deliverables: Periodically published EPA reports and professional literature

Timeline: Short to medium term

[20] EPANET is public-domain EPA software that models water distribution piping systems.

Challenge Area 4: Next-Generation Building Materials and Applications for Transportation Infrastructure Systems

Vision Statement

Build a resilient, sustainable, adaptable, and durable smart transportation infrastructure that incorporates high-performing materials, optimized structural designs, advanced sensor systems, and fabrication and construction processes that meet mobility and livability challenges

Introduction

To achieve this vision, R&D is needed to adapt innovative building materials and processes to practical engineering applications to improve the aging transportation infrastructure; and to develop next-generation building materials and engineering processes that result in revolutionary technologies to enhance the resilience of future transportation infrastructure.

Transportation systems are essential for the Nation's national security and economy. The transportation sector enables commerce, provides evacuation routes during emergencies, provides mobility, and connects communities. The system is complex, consisting of roads, highways, and bridges; railways; airports; pipelines; navigable waterways; and inland and sea ports. Disruptions to any of these networks have cascading effects. As an identified lifeline function, a secure and resilient transportation system is essential for the operation of other critical infrastructure sectors.

Much of the physical transportation infrastructure in the United States is aging, making the system increasingly vulnerable to disruptions as structures exceed their design lives. The Nation's transportation system faces a backlog of maintenance and reinvestment needs. Additionally, there are new and evolving hazards in the sector such as extreme weather events, terrorism, and other hazards that may negatively affect network performance. Compounding these problems, road systems are handling increasingly higher volumes of traffic carrying increasingly heavier loads, causing roads and bridges to wear more rapidly.

R&D is needed to refine infrastructure design and processes incorporating next-generation materials to provide high-performance, low-maintenance structures that are resilient, safe, and reliable under all conditions of service, including extreme events. These materials must also be easily adaptable to anticipate future requirements. Discoveries in material sciences and the development of new manufacturing, construction, and design processes have led to advances in building technology, such as longer-span bridges, better pavement surfaces, and safer and more durable structures. Continued R&D investment in innovative materials and design concepts will help the Nation build resilient transportation systems and repair or rehabilitate existing systems to extend their useable lives. Improved methods and technologies for evaluating the condition of infrastructure will also increase diagnostic capabilities and assist in prioritizing investments.

Goals

To address Challenge Area 4, the Federal Government should pursue the following four goals for CISR R&D for critical transportation infrastructure:

4.1. Modernized critical transportation infrastructure

4.2. Transportation infrastructure that withstands extreme events

4.3. More rapid, efficient and cost-effective building and repair of transportation infrastructure

4.4. Diagnostic capabilities for assessing the performance and condition of infrastructure

4.1. Modernized Critical Transportation Infrastructure

A modern transportation infrastructure designed to reduce operational and replacement costs and provide extended service life is a necessity. Fewer states of disrepair, lower cost of maintenance, fewer disruptions to travel time, and faster recoveries after disruptions reduce social and economic losses. Materials, designs, and construction practices need to be developed that require minimal or no maintenance over the duration of a bridge life expectancy of at least 100 years and pavement life expectancy of at least 50 years.

4.1.1. Develop, pilot, and support research on next-generation building materials to ensure extended performance by addressing strength, durability, and life-cycle requirements to improve the condition and performance of transportation infrastructure. DOT, DHS, NSF, and USACE will work with other agencies to support or coordinate these R&D activities.

Deliverables: Stronger, more ductile, and more corrosion-resistant steels; advanced paint systems and coatings; stronger, durable, flexible, and crack-resistant concretes; concrete mixes that use less Portland cement and more crushed limestone; corrosion-resistant reinforcing bars and strands; decay-resistant wood and wood products; more durable asphalts; nanomaterials; and polymers for infrastructure applications.

Timeline: Medium term to long term

4.1.2. Develop and adapt building materials for challenging environments, including cold weather or underwater, to improve the integrity of levees, flood walls, bridge piers, and other underwater structures. USACE and DOT will work with other agencies to coordinate this activity.

Deliverable: Faster hardening concretes and cements

Timeline: Medium term

4.1.3. Develop new mechanisms for locks, flood gates, and pumps that are more durable, less costly, and more reliable to reduce potential damage from hurricanes and flooding. USACE will work with other agencies to coordinate this activity.

Deliverable: New designs for locks, flood gates, and pumps that meet these criteria

Timeline: Long term

4.1.4. Improve quality control management systems for the construction industry to enable certification of steel quality, which will improve predictions of reliability for bridges and railroads. NIST will work with other agencies to coordinate this activity.

Deliverable: Certified reference materials to enable certification of steel quality

Timeline: Short term

4.2. Transportation Infrastructure that Withstands Extreme Events

Extreme events can severely disrupt transportation systems, often intensified by the poor initial condition of the infrastructure. Additionally, not all hazards are addressed in current codes and specifications, nor is technical understanding at the same level across all hazards. The continuing threat of terrorism has created a need to address vulnerability of the system to blast damage. The impacts of extreme weather events also threaten transportation network performance, and, if not addressed adequately, infrastructure failures may become more frequent and more catastrophic as the intensity and frequency of weather events increase. The challenge for the built community is to understand system vulnerabilities and develop methodologies so that damage from an extreme event does not disrupt transportation services. The development and adaptation of advanced and smart materials, optimized designs addressing extreme events, and performance-based codes and standards will contribute to minimizing vulnerability and achieving a more resilient transportation infrastructure.

4.2.1. Develop and pilot innovative bridge systems using smart materials (such as materials with memory) that greatly minimize or eliminate damages following an earthquake or other dynamic events. DOT will work with other agencies to coordinate this activity.

Deliverable: Designs for bridges and other transportation structures that are more resilient to dynamic loads, materials that can record stress history in infrastructure applications, and systems that return to their original position or shape after an event

Timeline: Medium term to long term

4.2.2. Combine high-performing materials to create new applications and designs to redirect and handle extreme event loads such as blast loads. DOT, USACE, and DHS will coordinate this activity.

Deliverable: New material combinations that are lightweight and yet effective in mitigating blast hazards, to be used for retrofitting existing structures or for use in new designs

Timeline: Medium term to long term

4.2.3. Develop performance-based designs addressing all hazards. DOT will work with other agencies to coordinate this activity.

Deliverable: New performance-based design standards and specifications addressing flooding and scour, seismic, blast, wind, fire, and other extreme events for transportation structures

Timeline: Medium term to long term

4.2.4. Develop retrofit designs that preserve infrastructure based on previously-unaccounted for environmental conditions, such as sea-level rise and extreme weather events. DOT and USACE will work with other agencies to coordinate this activity.

Deliverable: New designs and design modifications that preserve existing infrastructure in the face of sea-level rise and weather events

Timeline: Short term

4.2.5. Develop optimized bridge shapes to minimize hazard impact. DOT will work with other agencies to coordinate this activity.

Deliverable: Aero-elastic designs that mitigate wind loadings, hydrodynamic designs that mitigate hydraulic loadings, and structural shapes that mitigate blast loadings.

Timeline: Short to medium term

4.2.6. Refine dampers and damping systems to minimize the impact of dynamic loads and vibrations. DOT will work with other agencies to coordinate this activity.

Deliverable: New damping systems that handle wind, seismic, blast, impact, and other dynamic loads on structures

Timeline: Medium to long term

4.3. More Rapid, Efficient and Cost-Effective Building and Repair of Transportation Infrastructure

Delays and disruptions to traffic flows due to construction and maintenance add to the cost of travel and strain public goodwill. As transportation systems are rarely shut down completely for maintenance and construction, work often takes place alongside traffic, which endangers work crews. Timely and efficient repair of infrastructure, especially following extreme events, is crucial for maintaining both the functionality of the transportation system and the public's safety. The cost of traffic disruptions will also decrease if repairs are completed more rapidly.

4.3.1. Develop designs that incorporate modularity with adaptive capability to adjust to changing demands over the life of the infrastructure. DOT will work with other agencies to coordinate this activity.

Deliverable: New modular concepts in bridge and roadway designs that can be built rapidly, and applied to new projects to meet changing requirements to meet changing requirements

Timeline: Medium to long term

4.3.2. Develop rapid quality assurance testing procedures and acceptance tests. NIST will work with other agencies to coordinate this activity.

Deliverable: New electrical test methods for fresh concrete that provide rapid feedback on construction process quality

Timeline: Short term

4.3.3. Improve the efficiency and reliability of construction practices used to build and repair transportation infrastructure. NIST will work with other agencies to coordinate this activity.

Deliverable: Measurement science that assesses the ability to pump concrete mixtures to avoid costly blockages from aggregates "clumping."

Timeline: Short term

4.3.4. Research bonding properties and mechanisms between dissimilar materials. NIST and DOT will work with other agencies to coordinate this activity.

Deliverable: Compatible materials for engineering applications

Timeline: Short term

4.4. Diagnostic Capabilities for Assessing the Performance and Condition of Infrastructure

To properly maintain transportation infrastructure, especially roadways and bridges, better information is needed in a timely manner to determine the condition of materials and structures. Better information garnered from sensors will improve diagnostic capabilities and help transportation authorities prioritize repairs and determine when to intervene, preventing failure and lowering costs for maintenance and repairs.

4.4.1. Develop new or refine existing sensors that are reliable, durable, interchangeable, and effective in determining z are effective for multiple hazards such as seismic, aerodynamic, hydrodynamic, blast, fire, and other hazards; (2) sensors that can ascertain deterioration in concrete, steel, and pavements; (3) sensors that can determine material quality; and (4) sensor systems that can be easily updated or switched in place.

Timeline: Medium to long term

4.4.2. Integrate remote sensing space-based observation systems with ground sensors and smart materials to identify and reduce vulnerabilities and to assess the condition of transportation lifelines especially during and after a hazard event. DOT will work with other agencies to coordinate this activity.

Deliverable: Technology to use space-based observation systems for performance and condition assessment.

Timeline: Medium term

Challenge Area 5: Resilient and Secure Energy Delivery Systems

Vision Statement

Develop technologies, models, and analytic tools that enable energy owners and operators to design, implement, operate, and maintain secure and resilient energy delivery systems that are capable of sustaining critical functions during and after disruptive events.

Introduction

This vision will be achieved by implementing technology strategies that improve the reliability, resilience, and security of modern energy delivery systems, while mitigating risks associated with cross-sector interdependencies within the context of a dynamic energy system transformation.

Responsibility for energy security and resilience is shared between industry and government. Accordingly, R&D efforts in the Federal Government are coordinated with private-sector counterparts as part of a robust national strategy. The private sector has the primary responsibility for developing, deploying, and implementing risk reduction technologies and practices; the Federal Government supports these efforts by conducting fundamental, enabling, and applied R&D in areas such as novel technologies and materials, integrated planning tools, computational and simulation models, analysis of complex systems, and foundational science and engineering discoveries.

Energy delivery systems encompass diverse and geographically dispersed physical, cyber, and cyber-physical assets used to deliver power, fuels, and energy products through electricity, oil, and natural gas infrastructures. These systems support the production, refining, storage, and distribution of oil, gas, and electric power. R&D is needed to design, build, and operate energy delivery systems that can anticipate, prevent, and minimize disruptions, and recover rapidly when disruptions occur.

Federal R&D is focused on creating resilient and secure energy delivery systems that have the following characteristics: 1) an electric transmission system that can detect fluctuations and disturbances in the bulk power system and quickly and automatically compensate for conditions to prevent or minimize outages; 2) self-healing electric transmission and distribution systems that can automatically isolate faults and restore power to most customers using networked automated devices, support safe operation of islands and microgrids, and pinpoint the locations of damage to help accelerate restoration; 3) resilient control systems operating throughout the energy delivery system (electric, oil, and natural gas) with strong physical and cyber security and secure and redundant communication services; and 4) a portfolio of enabling technologies, such as energy storage, robust communications networks, alternative or redundant systems, and microgrid operations, which increase the continuity of energy services to end users and mitigate cross-sector impacts.

Goals

The following six goals guide Federal R&D efforts to achieve the vision for Challenge Area 5:

- 5.1. System design for resilience
- 5.2. Preparedness and mitigation measures
- 5.3. System response and recovery
- 5.4. Characterization and management of energy interdependencies
- 5.5. Energy systems that withstand high-impact, low-frequency events
- 5.6. Next-generation cyber-physical security capabilities

The following activities describe ongoing and prospective Federal R&D activities that support private-sector efforts and are expected to generate the outputs needed to achieve CISR R&D goals for the energy sector.

5.1. System Design for Resilience

Pursue innovative R&D on enhanced sensing and control technologies to better detect disturbances, automatically respond to and mitigate cascading effects, and minimize impacts to end users.

5.1.1. Conduct R&D to improve measurement, sensing, and real-time wide-area visibility of transmission grid behavior using phasor measurement units (PMUs) and synchrophasor data, and develop advanced communications and control systems, next-generation PMUs and software applications, and PMU-based algorithms needed to identify and react to disturbances and enable self-healing systems and automatic islanding. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Advanced communications and control systems, next-generation PMUs and software applications, and PMU-based algorithms that identify and react to disturbances and enable self-healing systems and automatic islanding.

Timeline: Medium term

5.1.2. Develop innovative grid modeling approaches that improve computational speeds by several orders of magnitude and validate power system models in real-world environments using real-world data. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Advanced computational and modeling capabilities, including dynamic operation, real-time analysis, and predictive response, that can be tested to simulate power system behavior in a real-world environment

Timeline: Short term

5.1.3. Develop advanced, secure, low-cost sensors and advanced distribution management system applications in order to enable full integration of distributed energy resources and microgrids. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Demonstration and validation of low-cost sensors for advanced distribution management system applications

Timeline: Short term

5.1.4. Develop cost-competitive next-generation grid-scale energy storage systems with improved power conversion and control technologies. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: An energy storage system that can compete with current peak generation resources on a cost-benefit basis

Timeline: Medium term

5.1.5. Develop a resilience metrics framework that serves as a decision support tool for identifying mitigation investment options against various hazards (physical and weather-related). DOE, in collaboration with DHS, will coordinate this activity.

Deliverable: A resilience metrics framework that can serve as a decision support tool.

Timeline: Short term

5.1.6 Support research and development on modeling and analysis of power grids and interdependent energy infrastructures, associated communication networks, contingency analysis, cybersecurity analysis, and fault detection and isolation methods. NSF will support this activity with other departments and agencies, as appropriate.

Deliverable: Models of power grids that can be employed to assess the resilience of communication networks and security from cyberattacks for an existing regional grid.

Timeline: Long term

5.2. Preparedness and Mitigation Measures

Develop new tools for resilience assessment, identifying and monitoring failure modes of energy equipment and systems (such as power system equipment, synchrophasors and frequency disturbance recorders, and multi-sensor data concentrators used to monitor conditions of power delivery networks for both transmission and distribution), and damage prediction models. Improve flexibility and robustness measures such as electronic-based power controllers, energy storage, and microgrids.

5.2.1. Enhance and implement risk management tools, such as the Cybersecurity Capability Maturity Models and Risk Management Process, to improve cybersecurity risk management practices among energy providers. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Pilot Cybersecurity Capability Maturity Models data analytics and benchmarking methodologies with utility volunteers, building on existing benchmarking work.

Timeline: Short term

5.2.2. Develop and implement a virtual collaborative environment for conducting rapid advanced digital forensics and malware analysis for the energy sector to detect and mitigate malicious activity, including safe analysis of malware, zero-day vulnerabilities, and advanced threats. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: A self-sustaining virtual collaborative forensics platform

Timeline: Short term

5.2.3. Develop and implement a smart grid interoperability test bed to enable accurate measurements of sensors (phasor measurement units, merging units, smart meters, and other distribution sensors) and distribution system and microgrid components (microgrid controllers, inverters, and other equipment) under dynamic grid conditions appropriate to resilience scenarios, and to characterize and validate interoperability of microgrid and other smart grid equipment. NIST will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: A test bed to characterize smart grid systems and sensor performance, standards, and interoperability, including microgrid controllers and phasor measurement units, under dynamic grid conditions representative of resilience scenarios

Timeline: Short term

5.2.4. Develop models, methodologies, and test beds for monitoring energy networks and for automatic responses to contingencies both natural and deliberate. Emphasis will be on evolving current theory and methodologies to be applicable to the future power grid with a growing penetration of renewable energy sources and independent producers. NSF will coordinate this activity, with additional promotion and coordination from other agencies.

Deliverable: A test bed for modeling automatic response in a complex grid environment

Timeline: Long term

5.3. Energy System Response and Recovery

Improved situational awareness and resilient communications systems that will speed response and recovery and strengthen resilience. Other R&D areas include new energy management systems and optimization tools for restoration prioritization.

5.3.1. Improve situational awareness through the Cybersecurity Risk Information Sharing Program (CRISP), facilitate timely sharing of threat information, and enhance the energy sector's ability to identify threats and coordinate protection of critical infrastructure. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: CRISP Operational Pilot with advanced analytical capabilities to enrich the participant's data with U.S. Government information that improves the effectiveness in identification of threats

Timeline: Short term

5.3.2. Conduct research on advanced system modeling and behavior analysis in various operating conditions (normal, alert, emergency, and restorative states) as well as in system operational procedures and automated tools to manage and protect interconnected energy systems under contingencies. NSF will coordinate this activity, with additional promotion and coordination from other agencies.

Deliverable: Models and automated tools that manage and protect interconnected energy systems under contingencies.

Timeline: Long term

5.4. Characterization and Management of Energy Interdependencies

Build a comprehensive framework for modeling and simulating cross-sector interdependencies by integrating multiple disparate models and simulations to conduct cross infrastructure analysis that addresses threat assessment, preparedness, mitigation, response, and recovery issues. Such a framework should have the ability to evaluate complex systems to help ensure that integrated energy infrastructures do not have hidden failure modes.

5.4.1. Conduct predictive analytics on interconnected energy infrastructure systems to predict future system performance. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Pilot-ready analytical products that incorporate advanced predictive analytics (to include understanding of how historical asset performance affects overall system performance) to improve decision making.

Timeline: Short term

5.4.2. Develop models and methodologies that facilitate fundamental research on interdependencies in interconnected energy infrastructure systems. NSF will coordinate this research, with additional promotion and coordination from other agencies.

Deliverable: Models that can be applied to a regional grid that identify interdependencies with other energy systems.

Timeline: Long term

5.5. Energy Systems that Withstand High-Impact, Low-Frequency Events

Develop and explore critical technologies and components that allow energy delivery systems, particularly the bulk power system, to withstand the consequences of a variety of high-impact, low-frequency incidents, such as geomagnetic-induced currents, geomagnetic disturbances (GMDs), electromagnetic pulses (EMPs), and other physical threats to critical grid components.

5.5.1. Expand modeling and testing of transformer vulnerabilities to GMD/EMP by including critical components, such as circuit breakers and relays, develop prototypes of next-generation transformers with enhanced flexibility and functionality, and evaluate designs for improved resilience. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: Next-generation transformer designs that are more standardized, more adaptable, and more interoperable between systems relative to current systems.

Timeline: Long term

5.5.2. Develop a decision support capability for providing utility operators with tailored forecasts of space weather effects on local power grids. DHS, in coordination with the Department of Commerce, will coordinate this activity.

Deliverable: Space weather forecasts with actionable information that assist in making operational decisions to mitigate effects to the grid from space weather

Timeline: Long term

5.6. Develop Next-Generation Cyber-Physical Security Capabilities

Develop and demonstrate next-generation cyber-physical security capabilities to address continually evolving cyber-physical threats, the introduction of new power system technologies, and the use of legacy devices in ways not previously envisioned.

5.6.1. Conduct high-risk, high-payoff energy delivery control system cybersecurity research, and medium-term R&D, to strengthen and maintain core capabilities for the energy sector, including technologies or techniques that identify, encapsulate, and remove undesired functionality inserted into an energy control system or component at some point along the supply chain. DOE will coordinate this activity with other departments and agencies, as appropriate.

Deliverable: By 2020, designs and piloting of resilient energy systems to survive a cyber incident while sustaining critical functions.

Timeline: Medium term

5.6.2. Model and analyze cyber-physical vulnerabilities of energy systems. NSF will support efforts on research on fundamental issues pertaining to physical aspects of cybersecurity.

Deliverable: Cybersecurity models that replicate the behavior of new power system technologies and legacy devices in the face of evolving cyber threats.

Timeline: Long term

Non-Federal Stakeholder R&D Activities

The previous sections describe Federal activities that will contribute to making the Nation's critical infrastructure more secure and resilient through R&D. Each section describes a vision for one of five Challenge Areas that can be fully realized through a coordinated effort on the part of the Federal Government and non-Federal stakeholders. Non-Federal efforts that complement the goals described for each of the Challenge Areas are summarized here to highlight the current role of non-Federal R&D stakeholders in these activities.

Challenge Area 1: Understanding Interdependencies in Infrastructure Vulnerabilities for Improved Decision Making

Current R&D with respect to CISR in the private sector is mostly confined to work within specific infrastructure sectors. This is due in part to the sector-specific focus of the owners and operators of infrastructure. An additional constraint is that there are significant barriers to data sharing within the private sector and between the private sector and public sector.

The public policy and planning support focus of this Challenge Area could be considered inherently governmental in its scope and goals; the private sector has limited financial or regulatory incentive to participate in developing those tools. This is exacerbated by the long planning horizons of the public investment decisions, which are outside the economic return on investment horizons of most private firms. Despite these obstacles, stakeholders do conduct R&D on behalf of and with Federal Government entities regarding interdependencies. These activities span the goals described for this Challenge Area.

Challenge Area 2: Position, Navigation, and Timing Support Functions

Federal R&D with respect to PNT can be transitioned into the private sector, and opportunities exist for private-sector stakeholders to conduct R&D in support of the goals described for this Challenge Area. In Goals 2.1 and 2.2 for this Challenge Area, private-sector stakeholders are identified as potential partners to complete specific R&D activities, and these are specific areas for which private-sector stakeholders can seek to engage with the Federal Government.

Private-sector companies are already developing technologies that can support and augment Federal activities. For example, many scalable, reliable, and secure components and complete timing systems are being developed by manufacturing companies. Additionally, a major role of the private sector will be to incorporate hardware changes and recommendations into PNT receivers that are mass produced, such as those in cell phones, so that users are using the latest generation of assured PNT receivers. Telecommunications, information technology, and financial industries are interested in increasing resilience and security of timing systems for the operation of their infrastructures, and these enhancements go hand in hand with national critical infrastructure improvements.

Challenge Area 3: Resilient, Secure, and Modernized Water and Wastewater Infrastructure Systems Capable of Integration with Legacy Systems

Many nonprofit organizations within the water and wastewater sector are conducting and funding research that addresses the goals outlined for this Challenge Area. For example, some research funded by private-sector stakeholders addresses emergency preparedness, resilience and sustainability, chemical alternatives, drought, vulnerability assessments, detection, and cybersecurity. Additional areas of private-sector research related to the goals of this Challenge Area include the impacts of extreme weather events, compounds of emerging concern, pathogens and human health, security and emergency response, and sensor technologies.

In addition to novel R&D efforts, several sector-specific organizations develop standards and also administer certification programs they have developed both through internal research efforts and reviews of external research publications to inform private-sector owners and operators. Standards developed by these private-sector partners cover topics such as drinking water treatment and distribution products, water storage and reservoirs, materials, equipment, and practice for water treatment and supply, and guidance on operations and management of municipal water facilities. Currently, Federal agencies, such as the EPA, engage with non-Federal stakeholders regularly, which allows for coordination of CISR R&D activities among the different stakeholders associated with this Challenge Area.

Challenge Area 4: Next-Generation Building Materials and Applications for Transportation Infrastructure Systems

Some non-Federal stakeholders perform transportation-sector R&D supported by funds from Federal, State, and nonprofit organizations. The R&D activities of these organizations are complementary to the goals described for this Challenge Area and include improving materials for transportation systems, transportation infrastructure resilience to extreme events, bridge construction methods, and diagnostic capabilities. In addition, State highway agencies use their portion of the State Planning & Research funds to support applied research activities.

Industry in the transportation sector most actively pursues R&D to improve products. Chemical, steel, cement, and concrete manufacturers conduct research to improve their products, although in most cases the results remain proprietary. Commercial companies collaborate with infrastructure owners and operators to ensure that their products are developed with practical applications.

Challenge Area 5: Resilient and Secure Energy Delivery Systems

Nearly all of the equipment and systems employed in energy delivery systems are developed and manufactured by the private sector. For example, the large and diverse electric power equipment and systems industry draws upon basic and applied research funded by Federal agencies, but the commercial products are designed and produced by equipment manufacturers and vendors in the private sector. In general, industry R&D of energy systems tends to be more short term compared to R&D funded by the Federal Government.

In addition to R&D conducted by industrial equipment manufacturers, energy sector owners and operators fund a substantial amount of R&D relating to the generation, delivery, and use of electricity for the benefit of the public. This research provides both short- and long-term solutions that enable the transformation of power systems to be more flexible, resilient and connected.

Conclusion and Next Steps

The Implementation Roadmap represents a coordinated approach for the Federal government to strengthen and maintain secure, functioning, and resilient critical infrastructure through R&D. The Implementation Roadmap identifies opportunities to apply science and technology solutions to address the intentional, unintentional, and adversarial threats against the Nation's critical infrastructure. By specifying activities that will lead to improvements in the five Challenge Areas and identifying the responsible Federal agencies, this Implementation Roadmap will help decrease the vulnerabilities and strengthen critical infrastructure to withstand and rapidly recover from the effects of extreme events.

As stated in PPD-21, "the Plan should be issued every 4 years after its initial delivery, with interim updates as needed."[21] Future updates to the Roadmap will be coordinated with the updates to the Plan. The Challenge Areas identified in this Roadmap will be refined and updated based on the progress of the activities, identified science and technology (S&T) gaps, and the evolving threat environment.

Security and resilience of critical infrastructure can only be achieved through ongoing partnerships between the Federal Government and the non-Federal owners, operators, and users of critical infrastructure. This is particularly important when attempting to pilot and deploy new methods and technology to strengthen critical infrastructure. Critical infrastructure owners and operators will use findings from federally funded R&D to improve modelling and update protocols and mitigation strategies that improve security and resilience. This transfer of information and technology can be used as a measure of progress for more mature CISR R&D activities and is a benchmark for successful partnerships between the government and the private sector. The broader non-Federal critical infrastructure community of owners, operators, and stakeholders will continue to be engaged in the implementation of and updates to the Roadmap. Though the focus of this Roadmap is on the S&T and technical goals of R&D, the operational aspects (e.g., technology transfer, deployment, training, awareness, etc.) will also need to be addressed in coordination with critical infrastructure owners, operators, and stakeholders to ensure that S&T developments are accessible to the broader community and advance a crosscutting culture of CISR R&D collaboration. The Federal Government can work with SCCs, CIPAC, university and other partnerships, and other established mechanisms to announce, coordinate, and accomplish the activities set out in this Roadmap.

[21] PPD-21, "National Critical Infrastructure Security and Resilience R&D Plan."

References

Beck, Michael W., editor. *Coasts at Risk: An Assessment of Coastal Risks and the Role of Environmental Solutions*. United Nations University - Institute for Environment and Human Security (UNU-EHS), The Nature Conservancy (TNC) and the Coastal Resources Center (CRC) at the University of Rhode Island Graduate School of Oceanography. 2014. http://www.crc.uri.edu/download/SUC09_CoastsatRisk.pdf

Environmental Protection Agency (EPA), *Safe and Sustainable Water Resources: Research Action Plan 2016–2019.* November 2015. https://www.epa.gov/sites/production/files/2015-10/documents/strap_2016_sswr_508.pdf.

Environmental Protection Agency (EPA), *Homeland Security Research Action Plan 2016–2019.* November 2015. https://www.epa.gov/sites/production/files/2015-10/documents/strap_2016_hs_508.pdf

Executive Order 13636. *Improving Critical Infrastructure Cybersecurity*. February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Federal Cybersecurity Research and Development Strategic Plan. February 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. December 2013. https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

National Critical Infrastructure Security and Resilience Research and Development Plan. November 2015. https://www.dhs.gov/publication/national-critical-infrastructure-security-and-resilience-research-and-development-plan.

National Infrastructure Advisory Council Water Sector Resilience: Final Report and Recommendations. June 2016. https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf

National Space Weather Strategy. October 2015. https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf

National Space Weather Action Plan. October 2015. https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatheractionplan_20151028.pdf

Presidential Policy Directive 8 (PPD-8). *National Preparedness*. March 30, 2011. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

Presidential Policy Directive 21 (PPD-21). *Critical Infrastructure Security and Resilience.* February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Presidential Policy Directive 41 (PPD 41). *United States Cyber Incident Coordination*. July 26, 2016. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.*Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*. April 2015. http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf

100 Resilient Cities. "About Us." http://www.100resilientcities.org/about-us#/-_/. Retrieved 1 July 2016.

Abbreviations

AC	Alternating current
CIPAC	Critical Infrastructure Partnership Advisory Council
CISR	Critical Infrastructure Security and Resilience
COTS	Commercial Off-The-Shelf
CRISP	Cybersecurity Risk Information Sharing Program
CT	Contact Time
DC	Direct current
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOT	Department of Transportation
EMP	Electromagnetic Pulse
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
GMD	Geomagnetic Disturbance
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSA	General Services Administration
HHS	Department of Health and Human Services
IDM	Interference Detection and Mitigation
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PMU	Phasor Measurement Unit
PNT	Position, Navigation, and Timing
PPD	Presidential Policy Directive
R&D	Research and Development
S&T	Science and Technology
SCC	Sector Coordinating Council
SSA	Sector Specific Agency
TIH	Toxic Inhalation Hazard
USACE	United States Army Corps of Engineers
USDA	United States Department of Agriculture