Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

February 4, 2022

# Extreme Weather and Lifeline Infrastructure Resilience: Provisions in the Infrastructure Investment and Jobs Act (IIJA)

On December 10, 2021, deadly tornadoes struck Kentucky, Arkansas, Tennessee, Missouri, and Illinois, killing nearly 90 people and causing widespread damage to lifeline infrastructure in the transportation, energy, water and wastewater, and communications sectors. (The Department of Homeland Security designates lifeline sectors as those where reliable operations are essential to many other critical infrastructure functions.) Many public officials and policymakers voiced concerns that the tornadoes and other extreme weather events represented a "new normal" of elevated risk to critical infrastructure.

The Infrastructure Investment and Jobs Act (IIJA; P.L. 117-58) directly funds resilience and adaptation projects for certain lifeline infrastructure. In addition, it makes new investments in research and development (R&D), analysis, and planning, which are intended to improve the critical infrastructure risk management practices of federal agencies and partners. This In Focus summarizes IIJA risk management provisions that address resilience of lifeline critical infrastructure sectors to extreme weather. Further, it discusses how implementation of these provisions may affect the national critical infrastructure security and resilience (CISR) enterprise as a whole.

## Policy Background

Federal agencies commonly assess risk as "a measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence." The statutory definition of critical infrastructure in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act (P.L. 107-56) incorporates this concept of risk—i.e., "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety."

As a discipline, critical infrastructure risk management focuses on identifying critical systems, assets, and networks; assessing vulnerabilities, threats, and hazards; and mitigating risk based on cost and other factors. The federal CISR policy framework consists of both compulsory (regulatory) and voluntary (non-regulatory) elements for managing risk, which coexist with—and often mutually influence—each other. Federal, state, local, territorial, and tribal (FSLTT) agencies, private sector stakeholders, researchers, and nonprofits manage critical infrastructure risks within this broad framework.

### Voluntary Public-Private Partnerships

Key federal nonregulatory authorities for voluntary CISR risk management programs date to the late 1990s. After the September 11, 2001, terrorist attacks, Congress enacted the Homeland Security Act of 2002 (P.L. 107-296), which expanded certain authorities and added others.

A 2013 presidential directive established 16 critical infrastructure sectors encompassing functions in industry, commerce, governance, and public safety. It assigned responsibility for leadership and interagency coordination to the Secretary of Homeland Security. Designated federal agencies and sector stakeholders have formed interagency, FSLTT, and private sector coordination bodies and information sharing organizations for each critical infrastructure sector and related subsectors.

Observers have offered mixed assessments of effectiveness, especially in the area of information sharing between the private sector and federal agencies. Private sector concerns about protecting proprietary information and avoiding potential legal exposure or regulatory enforcement have generally limited interest in information-sharing activities, despite enactment of certain legal exemptions and measures to protect confidentiality.

### Standards Development and Regulation

Standards for reliability and resilience of infrastructure systems, assets, and networks play a large role in critical infrastructure risk management. Private sector entities commonly develop and adopt voluntary consensus standards for reasons of business continuity, systems compatibility and interoperability, and public policy concerns—i.e., to preempt or complement regulatory mandates. Private sector entities develop standards both independently and in collaboration with FSLTT agencies.

Regulatory agencies may incorporate consensus industry standards by reference, giving them legal effect, or may allow covered entities to choose for themselves which—if any—elements of a given standard to adopt. Regulatory agencies may also create and enforce reliability standards independently as part of an existing regulatory process if authorized to do so by law.

Resilience and reliability standards for lifeline infrastructure against extreme weather hazards are largely voluntary outside the electricity subsector. In the case of the electricity subsector, a private nonprofit operating under auspices of the Federal Energy Regulatory Commission creates and enforces mandatory and enforceable standards in consultation with government and industry partners.

## Lifeline Sector Resilience and the IIJA

IIJA provisions for management of weather-related lifeline infrastructure risks apply to the transportation, energy, and water and wastewater systems sectors. Communications provisions focus on availability and affordability of broadband internet service.

### Transportation Systems Sector

IIJA establishes the Promoting Resilient Operations for Transformative, Efficient, and Cost-saving Transportation (PROTECT) Program to support adaptation and resilience projects, and improvement of planning and analysis functions (including vulnerability assessments). Funding from the Highway Trust Fund is authorized at an annual average of $1.7 billion over five years.

Further, IIJA authorizes a total of $500 million (subject to appropriation) for creation of 10 regional Centers of Excellence for Resilience and Adaptation. Examples of eligible activities include standards development for design, operations, and maintenance of climate-resilient transportation infrastructure; stakeholder engagements to increase technical capacity for risk assessments; and development of transportation infrastructure strategies with key stakeholders for long-term climate resilience. Under a separate provision, IIJA establishes the Advanced Research Projects Agency–Infrastructure (ARPA-I) within the Department of Transportation (DOT) to support R&D for infrastructure resilience, among other purposes. Funding is authorized subject to appropriation.

IIJA also mandates certain transportation data collection, management, and analysis activities. It requires DOT—in consultation with designated research centers and other stakeholders—to develop quantitative measures of resilience and annual risk affecting transportation infrastructure. Further, DOT must conduct outreach to governmental and nongovernmental stakeholders to assist in implementation of the new analytical methods and capabilities. DOT must also assist state and local jurisdictions and planning bodies in improving statistics to inform transportation policy, including infrastructure resilience to severe weather. IIJA authorizes $50 million (subject to appropriation) to support this activity.

IIJA also makes changes to the federal highway program to improve adaptation and resilience. IIJA adds definitions of *resilience* and *natural infrastructure* to U.S.C. Title 23. It allows use of federal funds for "protective features" to mitigate the risk of recurring damage from extreme weather events. It allows up to 15% of the annual apportionment of National Highway Performance Program funding to be used for resilience of highways or bridges not part of the National Highway System.

### Energy Sector

Under the federal CISR framework described above, the energy sector has two subsectors: electricity, and oil and natural gas. Energy infrastructure provisions of the IIJA related to resilience and adaptation focus on electricity.

IIJA creates a $5 billion grant program for grid operators, generation facilities, and other related entities to prevent outages due to climate-related hazards, and to enhance resilience of the grid. Some eligible activities include burying power lines, implementing distributed grid technologies, and improving information sharing capabilities. Some funding prioritizes community benefit as predicted by community risk assessments.

IIJA also provides $5 billion in competitive grants to states and other entities for advanced transmission, energy storage, and distribution demonstration projects "to harden and enhance resilience and reliability" in collaboration with electricity infrastructure operators. In addition, IIJA modifies Department of Energy authorities for facilitating expansion of transmission capacity, which may increase grid resilience to extreme weather. See CRS Insight IN11821, *IIJA: Efforts to Address Electric Transmission for Reliability, Resilience, and Renewables*, by Richard J. Campbell.

### Water and Wastewater Systems Sector

IIJA authorizes $500 million for water and wastewater systems resilience grant programs, divided evenly. For systems serving fewer than 10,000 people, it supports infrastructure inventory and mapping projects. For larger systems, it supports planning, design, and construction projects. Applicants from larger systems must include an assessment of natural hazard risk when applying.

IIJA also authorizes $25 million for centers of excellence to support storm water control infrastructure R&D, and $50 million to support development of relevant standards and adoption of new technologies. See CRS Report R46892, *Infrastructure Investment and Jobs Act (IIJA): Drinking Water and Wastewater Infrastructure*, by Elena H. Humphreys and Jonathan L. Ramseur.

## Policy Implications

IIJA may strengthen the government position in public-private partnerships by expanding agency risk assessment and planning capabilities, and by increasing their capacities to directly fund resilience research, standards development, and projects. Agencies may support development of favored technologies, and require private-sector utilities and other entities seeking grant funding to submit risk-based vulnerability assessments of lifeline infrastructure systems—a step that may increase risk awareness. In addition, new risk metrics and standards developed under IIJA may affect infrastructure policies and plans. IIJA may also affect interagency and FSLTT relationships. For example, new DOT funding and authorities may elevate its profile and reach within the national CISR enterprise.

Through legislation and oversight, Congress may affect how—or if—new standards, metrics, and technologies for lifeline infrastructure resilience are promulgated, whether through voluntary adoption or regulation. Congress may also exercise oversight of new agency functions, evolving interagency and FSLTT relations, and public-private partnerships.

**Brian E. Humphreys**, Analyst in Science and Technology Policy

## Disclaimer