



# **METHODOLOGY FOR ASSESSING REGIONAL INFRASTRUCTURE RESILIENCE**

---

## **Lessons Learned from the Regional Resiliency Assessment Program**

JUNE 2021



June 2021

Critical Infrastructure Stakeholders:

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor. CISA works with Federal, State, local, tribal, and territorial officials, public and private sector owners and operators of critical infrastructure, and academia to defend against today's threats and build more secure and resilient infrastructure for the future. The threats we face—digital and physical, man-made, technological, and natural—are more complex, and the threat actors more diverse, than at any point in our history. CISA is at the heart of mobilizing a collective defense as we lead the Nation's efforts to understand and manage risk to our critical infrastructure. The programs and services we provide are driven by our comprehensive understanding of the risk environment and the corresponding needs identified by our stakeholders. We seek to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

The Regional Resiliency Assessment Program, established in 2009, addresses regional critical infrastructure systems and their operations. In the past 10 years, the program adapted to a changing risk environment, advanced the Nation's preparedness for disasters, strengthened regional partnerships between government and the private sector, and developed a mature approach to addressing the unique challenges to resilience present at this scale of infrastructure operations.

CISA's *Methodology for Assessing Regional Resilience* provides critical infrastructure security practitioners with a common framework and process for addressing complex infrastructure resilience issues. This proven approach is one that many partners can benefit from and can be tailored to their own needs. This assessment focuses on filling a knowledge gap by capturing practical knowledge gained from a decade of real-world experience conducting dozens of assessments.

I am pleased to share CISA's practices and proven methods with all of our partners, as we work together to secure today and defend tomorrow.

Sincerely,

A handwritten signature in black ink that reads "Dr. David Mussington".

Dr. David Mussington  
Executive Assistant Director  
Infrastructure Security  
Cybersecurity and Infrastructure Security Agency

# Table of Contents

ii	Acronyms and Abbreviations	47	Accessing Controlled Datasets
<b>2</b>	<b>Introduction</b>	48	Multi-organizational Facilitated Discussions
2	Goal	49	One-on-One Interviews
3	Structure	51	Structured Surveys and Assessments
3	Intended Audience	53	Exercises
4	Marking 10 Years of Accomplishment	55	Plan Reviews
<b>8</b>	<b>Part 1: Foundational Concepts of Resilience</b>	<b>56</b>	<b>Step 4: Analyze</b>
8	Background on Resilience	59	Adhering to Analytic Standards
8	Building Blocks of Resilience	59	Dependency Analysis
11	Convergence of the Cyber and Physical Dimensions of Infrastructure	65	Consequence Analysis
11	Impact of Dependencies and Interdependencies on Infrastructure Resilience	66	Threat and Hazard Analysis
15	Connecting the Concepts of Risk, Preparedness, Security, Continuity, and Resilience	70	Vulnerability Analysis
16	Importance of Thinking Regionally	71	Criticality Analysis
18	Challenges in Strengthening Regional Resilience	71	Comparative Analysis
22	Infrastructure Resilience Assessment and the Coronavirus Pandemic	72	Geospatial Analysis
<b>24</b>	<b>Part 2: Methodology for Assessing Regional Infrastructure Resilience</b>	74	System Diagramming
25	Engage Partners	77	Capability Analysis
<b>28</b>	<b>Step 1: Identify Problem</b>	77	Plans Analysis
28	Potential Sources for Regional Assessment Concepts	78	Data Aggregation
29	Past experience with real-world incidents	79	Network Analysis
29	Working groups and partnership organizations	82	Failure Analysis
29	Prior assessments, operational plans, and exercises	83	Modeling and Simulation
30	State and local hazard analyses and capabilities assessments	86	Decision Analysis
30	Threat identification by public and private partners	<b>88</b>	<b>Step 5: Document and Deliver Results</b>
31	National strategic priorities for risk management and infrastructure resilience	88	Documenting Results
31	Pre-existing awareness of shortcomings in infrastructure knowledge and resilience	89	Developing Courses of Action
31	Obtaining Buy-in	90	Presenting the Information
<b>32</b>	<b>Step 2: Design Assessment</b>	92	Sharing Results
32	Refining an Assessment Concept	92	Guiding Principles for Product Development
33	Moving from General Concepts to Specific Ideas	<b>94</b>	<b>Step 6: Promote Action</b>
34	Selecting the Topic	94	Managing Risk Through Resilience Enhancements
34	Defining Specific Knowledge Gaps	95	Example Actions to Enhance Regional Infrastructure Resilience
35	Articulating Desired Outcomes	95	Planning
36	Developing Research Questions	96	Capital Investments and Grant Submissions
36	Scoping Assessment Activities	97	Training
40	Research Planning Techniques	97	Exercises
<b>41</b>	<b>Step 3: Collect Data</b>	98	Tracking Progress
42	Information Security	<b>100</b>	<b>Tying It All Together</b>
45	Data Collection Methods	102	Regional Assessment of Nationally-critical Data Centers
45	Literature Review	104	Regional Assessment of Electricity, Transportation, and Communication Infrastructure
46	Open-source Research	106	Regional Assessment of Surface Transportation Systems
		108	Regional Assessment of Healthcare Supply Chains
		<b>112</b>	<b>Conclusion</b>
		113	Glossary of Key Terms

## Acronyms and Abbreviations

BRIC	Building Resilient Infrastructure and Communities	LES	Law Enforcement Sensitive
CEII	Critical Energy/Electric Infrastructure Information	NIPP	National Infrastructure Protection Plan
CISA	Cybersecurity and Infrastructure Security Agency	NPMS	U.S. DOT National Pipeline Mapping System
CSZ	Cascadia Subduction Zone	ORR	New York City Mayor's Office of Recovery and Resiliency
CVI	Chemical-terrorism Vulnerability Information	OT	Operational Technology
DHS	U.S. Department of Homeland Security	PCII	Protected Critical Infrastructure Information
DOT	U.S. Department of Transportation	PPD	Presidential Policy Directive
EMD	Emergency Management Division	RRAP	Regional Resiliency Assessment Program
FEMA	Federal Emergency Management Agency	SCADA	Supervisory Control and Data Acquisition
FOUO	For Official Use Only	SPR	Stakeholder Preparedness Report
GIS	Geographic Information System	SSI	Sensitive Security Information
HIFLD	Homeland Infrastructure Foundation-level Data	THIRA	Threat and Hazard Identification and Risk Assessment
HSEEP	Homeland Security Exercise and Evaluation program	TLP	Traffic Light Protocol
ISAC	Information Sharing and Analysis Center	USACE	U.S. Army Corps of Engineers
IT	Information Technology	USCG	U.S. Coast Guard

This document includes a series of tips, examples, and checklists intended to help stakeholders use this methodology



**TIPS** capture specific lessons learned from previous assessments or relevant guidance resources



**EXAMPLES** summarize how CISA used various approaches in real-world projects



**CHECKLISTS** identify key actions that should occur before proceeding to the next step of an assessment



# INTRODUCTION

- 2 Goal
- 3 Structure
- 3 Intended Audience
- 4 Marking 10 Years of Accomplishment

## Introduction

The The Cybersecurity and Infrastructure Security Agency (CISA) has conducted thousands of critical infrastructure assessments nationwide since DHS began operations in 2003. Included among these efforts have been assessments of the resilience of regional critical infrastructure systems through the Regional Resiliency Assessment Program (RRAP). Since 2009, CISA has conducted more than 100 of these regional assessments, exploring issues related to the resilience of energy, water, transportation, communications, and other infrastructure systems in partnership with federal, state, local, tribal, and territorial stakeholders, as well as private sector owners and operators. Figure 1 provides an overview of RRAP activities and outcomes since the program's creation. The RRAP is a voluntary program that uses a structured assessment approach to build on the risk management process outlined in the 2013 *National Infrastructure Protection Plan (NIPP)* and conceptualize projects, collect data, analyze information, and present options for improving regional infrastructure resilience. CISA has learned valuable lessons while conducting this array of RRAP projects across the Nation in terms of what is required for successful regional assessments of infrastructure, what the likely challenges are in these efforts, and how strategies for collaborative engagement can enhance the value of these assessments over the long term.

## Goal

The goal of this document is to distill lessons from more than 10 years of RRAP projects and articulate a generalizable, repeatable methodology for conducting voluntary regional infrastructure resilience assessments that stakeholders—including federal, state, local, tribal, and territorial governments and private sector owner and operators—can tailor and apply to their own needs.

While the methodology described in this document was refined through the RRAP, the application of its principles and techniques is intended to stretch far beyond this single program in the hopes of strengthening the capabilities of a wide range of organizations and entire communities and regions to assess, understand, and improve the resilience of critical infrastructure systems nationwide. CISA shares this focus on infrastructure resilience with many other government organizations and private sector groups that are likewise seeking approaches to examining and addressing complicated resilience challenges. This document is intended to complement the growing body of work on infrastructure resilience, filling a knowledge gap by capturing practical knowledge gained from a decade of real-world experience conducting dozens of assessments via the RRAP.



## Understanding the NIPP

DHS published the *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* in 2013. The plan outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. The document was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry. It provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes. Information about the NIPP is available here: [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

## Structure

This document includes two parts:

- **Foundational Concepts of Resilience** draws from policy and research sources to establish a common foundation for what resilience means in the context of critical infrastructure and why studying resilience at a regional level is an important activity for public and private partners.
- **Methodology for Assessing Regional Infrastructure Resilience** articulates core elements of a general, scalable methodology for assessing the resilience of critical infrastructure, and defining key processes and analytical techniques that can yield tangible and actionable options for enhancing resilience through voluntary, collaborative partnerships.

Following publication of this document, DHS will also release supplemental guidance for specific types of assessments. These installments will include a series of stand-alone annexes that address more specific topics related to assessing particular types of regional infrastructure systems (e.g., electric power systems, petroleum supply chains, healthcare product supply chains, communications networks, ports, and cybersecurity of water and wastewater systems). DHS will continuously identify new topic areas for exploration and add to this body of reference material.

This document provides: 1) a common theoretical foundation for what infrastructure resilience is; 2) a scalable approach for designing and conducting assessments of infrastructure resilience; and 3) tailored methods for specific infrastructure systems and topics. The document’s intent is not to provide step-by-step instructions for every element of an infrastructure resilience assessment, but rather to outline key principles; define a repeatable methodology that is applicable across different levels of government, the private sector, and all infrastructure sectors; and provide additional examples and resources that users can consult as they move forward with implementing voluntary regional assessments of infrastructure resilience.

## Intended Audience

The intended audience for this document is any organization with a stake in the resilience and security of critical infrastructure operations, including the following:

- State, local, tribal, and territorial governments seeking to understand the resilience of critical infrastructure in their areas of responsibility;
- Regional public-private partnerships that facilitate collaboration among infrastructure owners and operators in the private sector and government partners responsible for public safety and community planning;
- Private sector entities that own and operate infrastructure in communities nationwide and may participate in broader regional resilience efforts with other industry and government partners;
- Federal personnel who work continuously with private sector partners and government counterparts to further the mission of infrastructure security and resilience; and
- Researchers who are pursuing improved approaches to examining and addressing critical infrastructure resilience on a regional scale.

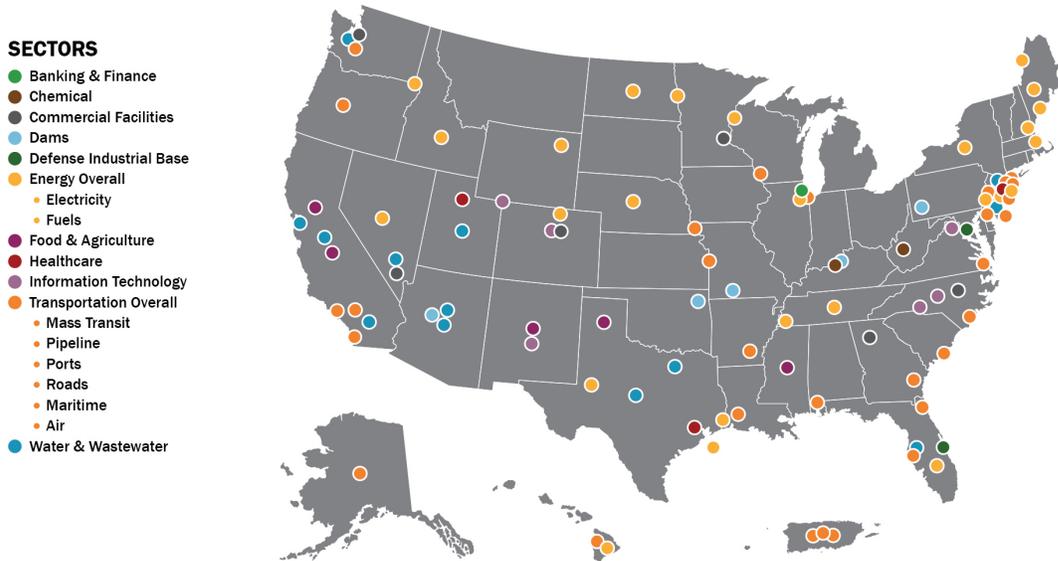
The types of organizations that could benefit from this methodology are diverse with distinct roles in the regional infrastructure resilience mission, and may have differing technical expertise, resources, and priorities. Nevertheless, all of these types of organizations could undertake the general type of assessment work described here based upon their respective capabilities and resources. As a result, this document is intended to inform all levels of assessment, from basic to intermediate to advanced.

# MARKING 10 YEARS OF ACCOMPLISHMENT

## REGIONAL RESILIENCY ASSESSMENT PROGRAM (RRAP): 2009–2019

### PROJECTS BY SECTOR

100 total projects across the continental U.S., Alaska, Hawaii, Puerto Rico, as well as Canada.



### THREATS AND HAZARDS

Projects explore different scenarios to understand impacts on infrastructure.

**NATURAL HAZARDS** 54 PROJECTS

- Storm surge/flooding
- Hurricane
- Earthquake
- Drought
- Climate change

**MAN-MADE HAZARDS** 26 PROJECTS

- Terrorism
- Intentional damage
- Hazardous materials
- Contamination events

**CYBER DISRUPTIONS** 21 PROJECTS

- Malware/Ransomware
- Denial of Service
- Data Breach
- Insider Threat
- Vulnerability exploitation

**INFRASTRUCTURE FAILURES** 8 PROJECTS

- Infrastructure outages
- Power outages
- Other utility outages

**100**  
RRAP Projects

**550**  
Infrastructure  
Asset Assessments

**51**  
Cyber  
Assessments

**1,700+**  
Partners

## OUTPUTS FOR STAKEHOLDERS

Projects generate a wide range of resources for use by stakeholders.



RESILIENCY  
ASSESSMENT  
REPORTS



COMPILED  
DATASETS



STATIC &  
INTERACTIVE  
MAPS



HAZARD  
IMPACT  
ANALYSES



PROCESS  
DIAGRAMS



INFOGRAPHICS



SYSTEM  
CONFIGURATION  
DIAGRAMS



TECHNICAL  
REPORTS



ECONOMIC  
IMPACT  
ANALYSES



DECISION  
SUPPORT  
TOOLS



SCENARIO  
PLANNING GUIDES  
& TEMPLATES

## KEY FINDINGS AND RESILIENCE ENHANCEMENT OPTIONS

Projects highlight analytic findings and potential courses of action for partners.

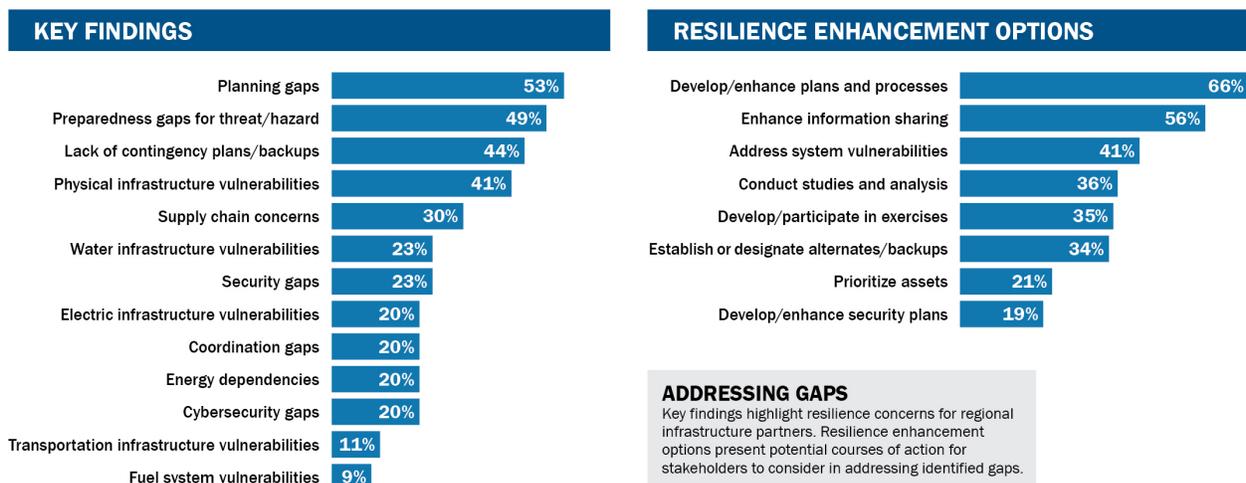


FIGURE 1.—Overview of DHS’s RRAP Efforts.

This page intentionally left blank.



## PART 1

# FOUNDATIONAL CONCEPTS OF RESILIENCE

- 8 Background on Resilience
- 16 Importance of Thinking Regionally
- 18 Challenges in Strengthening Regional Resilience
- 22 Infrastructure Resilience Assessment and the Coronavirus Pandemic

# PART 1 FOUNDATIONAL CONCEPTS OF RESILIENCE

## Background on Resilience

Although the concept of resilience has been applied in a variety of settings (e.g., psychology, psychiatry, ecology, social science, economy, and engineering) for several decades,<sup>1,2</sup> it has more recently received growing attention in the field of risk management. In particular, the critical infrastructure community has evolved from a primary focus on protective security in the 1990s to a broader emphasis on security and resilience.

In the homeland security domain, *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience* established national policy on strengthening and maintaining secure, functioning, and resilient critical infrastructure in sectors that are essential to the Nation’s security, public health and safety, economic vitality, and general quality of life.<sup>3</sup> The directive defined resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, including deliberate attacks, accidents, or naturally occurring hazards.<sup>4</sup>

The resilience of a community or region is a function of the resilience of its subsystems, including its critical infrastructure, economy, civil society, and governance. As outlined in the *Community Resilience Planning Guide* published by the National Institute for Standards and Technology, buildings and infrastructure play an important role in assuring the health and vitality of the social and economic fabric of the community.<sup>5</sup> Achieving resilience can be challenging due to the highly complex dependencies and interdependencies that exist within infrastructure systems, the geographic scale and jurisdictional boundaries across which infrastructure systems operate, the distributed ownership of

infrastructure, the distributed responsibility for risk management, and the potential for disruptions to cascade across systems.

Infrastructure resilience depends on both physical attributes of engineered infrastructure systems and on the capabilities of organizations affecting the operation and management of those systems (e.g., infrastructure owners and operators, regulatory authorities, vendors and contractors). Infrastructure resilience can be evaluated at the asset, system, or system-of-system levels. Resilience is also influenced by organizational factors such as the existence of business continuity and emergency response plans, the level of workforce training, frequency of exercises to test plans, flexibility in workforce scheduling, and internal and external communication capabilities.

## Building Blocks of Resilience

Definitions of resilience vary significantly by author and discipline. Some of these differences are rooted in the definition’s focus on a specific object (e.g., resilience of a facility; resilience of a system; resilience of a community). Other definitions of resilience highlight different time periods (i.e., resilience centering on measures taken before an incident versus after an incident). For the purposes of understanding the resilience of infrastructure from a regional perspective, the definition articulated in PPD-21 is a logical and widely used option. The core elements of that definition—the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions—can be characterized into four building blocks: preparedness, mitigation measures, response capabilities, and recovery

<sup>1</sup> Renschler, Chris S., Amy E. Fraizer, Lucy A. Arendt, Gian-Paolo Cimellaro, Andrei M. Reinhorn, and Michel Bruneau, “A Framework for Defining and Measuring Resilience at the Community Scale: The PEOPLES Resilience Framework,” *National Institute of Standards and Technology*. 2010. Accessed February 13, 2020. [www.hssl.org/?view&did=790013](http://www.hssl.org/?view&did=790013).

<sup>2</sup> Rose, Adam, *Economic Resilience to Disasters*, CARRI Research Report 8. 2009.

<sup>3</sup> White House, “Presidential Policy Directive – Critical Infrastructure Security and Resilience.” February 12, 2013. Accessed February 13, 2020. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

<sup>4</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>5</sup> NIST (National Institute of Standards and Technology), *Community Resilience Planning Guide for Buildings and Infrastructure Systems: Volume 1*, May 2016. Accessed February 13, 2010. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1190v1.pdf>.

mechanisms. These simplified bins are similar to the 2010 Quadrennial Homeland Security Review, the preparedness mission areas described by *Presidential Policy Directive 8 (PPD-8): National Preparedness*, and the subsequent *National Preparedness Goal*. Together, these four building

blocks can help practitioners deconstruct the concept of resilience into actionable steps and ultimately gauge progress in enhancing resilience over time. Table 1 describes these building blocks and offers examples for consideration.<sup>6</sup>

**TABLE 1**  
**Building Blocks of Resilience**

	Description	Examples
<b>Preparedness</b>	Activities undertaken to <b>anticipate</b> relevant threats/hazards and the possible consequences from their occurrence, including prevention and protection activities; speaks to the adaptability of infrastructure systems and the process of integrating and acting on lessons learned	<ul style="list-style-type: none"> <li>■ Maintaining security force</li> <li>■ Installing/monitoring physical access controls</li> <li>■ Developing continuity plans, emergency operations plans, and cybersecurity plans</li> <li>■ Training personnel on plans</li> <li>■ Conducting regular exercises to validate plans</li> <li>■ Establishing information sharing mechanisms</li> </ul>
<b>Mitigation</b>	Activities undertaken to <b>resist</b> and/or <b>absorb</b> the negative impacts of an event, reducing the severity or consequences of a hazard; speaks to the robustness of infrastructure	<ul style="list-style-type: none"> <li>■ Retrofitting facilities to mitigate the effects of different natural hazards (e.g., flood-proofing equipment, flood barriers)</li> <li>■ Upgrading equipment that will withstand anticipated hazards</li> <li>■ Improving the reliability/redundancy in supporting infrastructure systems</li> <li>■ Establishing an alternative backup site that can continue operating after an incident and facilitate restoration efforts</li> <li>■ Understanding cross-sector dependencies on key external resources (e.g., power, fuel, water, communications)</li> <li>■ Prestaging additional supplies (e.g., fuel, backup generators, backup communications)</li> </ul>

<sup>6</sup> Carlson, J. Lon, Rebecca A. Haffenden, Gilbert W. Bassett, William A. Buehring, Michael J. Collins, III, Stephen M. Folga, Frédéric Petit, Julia A. Phillips, Duane R. Verner, and Ronald Whitfield, *Resilience: Theory and Application*. 2012. United States. doi:10.2172/1044521. [www.osti.gov/biblio/1044521-resilience-theory-application](http://www.osti.gov/biblio/1044521-resilience-theory-application).

TABLE 1.—Building Blocks of Resilience (continued).

Description	Examples
<p><b>Response</b></p> <p>Activities and programs undertaken or developed to <b>respond</b> and <b>adapt</b> to the adverse effects of an event; speaks to the resourcefulness of infrastructure owners and operators in managing a crisis</p>	<ul style="list-style-type: none"> <li>■ Maintaining onsite response capabilities for key hazards (e.g., chemical spills, fires, explosives, armed assault, medical emergencies)</li> <li>■ Building relationships with local first responders and cross-sector partners</li> <li>■ Having onsite incident management capabilities, including trained personnel, a functioning operations center, and an understanding of cross-sector issues</li> </ul>
<p><b>Recovery</b></p> <p>Activities and programs designed to help entities return operating conditions to a level that is acceptable and <b>recover</b> from an event; speaks to the ability to get services back on line quickly</p>	<ul style="list-style-type: none"> <li>■ Establishing priority restoration agreements with key service providers</li> <li>■ Assessing the time and activities required to restore an organization to full operations following a disruption</li> <li>■ Rapid replacement/repair strategies for critical components (e.g., pre-certified suppliers, maintaining emergency supply)</li> </ul>

Another way to think about these building blocks of resilience is to conceptualize them in the context of infrastructure operations from a timing perspective, as illustrated in figure 2. Preparedness and mitigation measures are pursued before an event happens in order to help an organization anticipate what could happen, resist the effects of a negative event, and absorb

the impacts that arise in the aftermath. Response and recovery measures affect actions taken after an event occurs and triggers a disruption in normal operations. During these phases, activities center on helping an entity address the immediate effects of an event, adapt to a new operating environment, and recover core operations to the previous, or a new, equilibrium.

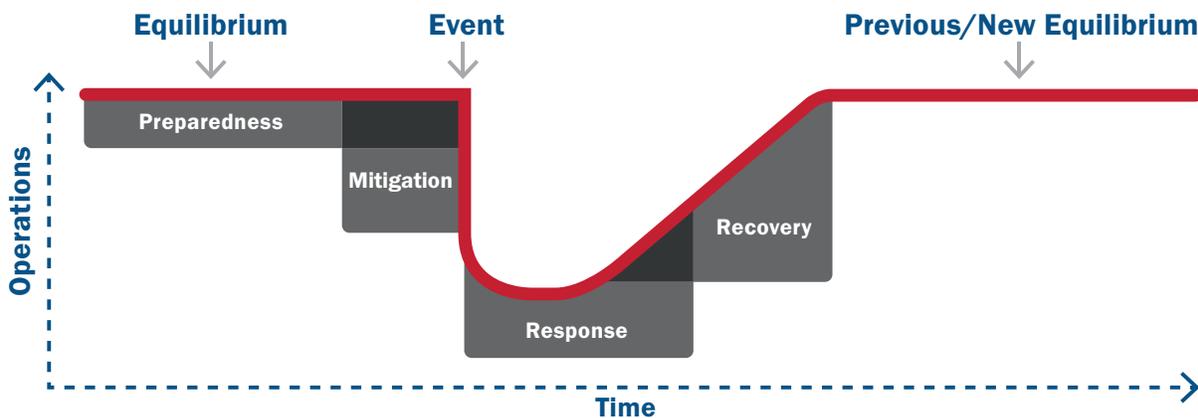


FIGURE 2.—Visualizing Resilience as a Curve.

## Convergence of the Cyber and Physical Dimensions of Infrastructure

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences all continue to evolve. Critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks; this development stems from the growing integration of information and communications technologies with critical infrastructure operations, and adversaries focused on exploiting potential cyber vulnerabilities.<sup>7</sup> The threat environment is dynamic, with an array of risks to infrastructure systems from nation-state adversaries and competitors, extreme weather events, and terrorism and violent crime. These risks are more numerous, complex, dispersed geographically and across stakeholders, and they are challenging to understand and manage. Infrastructure systems and the critical functions they enable are systems of systems with complex interdependencies and potential for cascading failures if disrupted.<sup>8</sup>

From an operational perspective, critical infrastructure across all sectors increasingly relies on both physical assets and cyber systems to function effectively. Today's threats are often hybrids that use physical infrastructure, information technology (IT), and operational technology (OT) as the avenue of approach for an adversary. For example, electric power systems involve both physical resources to generate and transmit power (e.g., generation plants, transmission towers, transmission and distribution power lines, transmission and distribution substations, control centers) and cyber systems to manage them (e.g., supervisory control and data acquisition [SCADA] systems to control remote operations, distributed control systems for process control at power plants, smart technologies for metering and status reporting). These physical

and cyber elements have distinct vulnerabilities to different threats and hazards and can generate a range of consequences if disrupted. They also increase the complexities associated with identifying and analyzing infrastructure dependencies and interdependencies.

## Impact of Dependencies and Interdependencies on Infrastructure Resilience

Growing dependencies and interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks.<sup>9</sup> A dependency is a unidirectional relationship between two assets where the operations of one asset affect the operations of the other. For example, a water treatment plant may depend on communications services that support the SCADA systems required to control plant operations. An interdependency is a bidirectional relationship between two assets where the operations of both assets affect each other. An interdependency is effectively a combination of two dependencies—therefore, understanding an interdependency requires analysis of the one-way dependencies that comprise it. For example, a water treatment plant could require communications for its SCADA system, and, in turn, provide water used by the communications system to cool its equipment. Figure 3 illustrates the definitions of dependency and interdependency.<sup>10</sup>

<sup>7</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>8</sup> CISA (U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency), *Strategic Intent: Defend Today, Secure Tomorrow*. August 2019. Accessed February 13, 2020. [www.cisa.gov/publication/strategic-intent](http://www.cisa.gov/publication/strategic-intent).

<sup>9</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>10</sup> Petit, Frédéric, Duane Verner, David Brannegan, William Buehring, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Philips, and James Peerenboom. *Analysis of Critical Infrastructure Dependencies and Interdependencies (ANL/GSS-15/4)*. 2015. Retrieved from Argonne, Illinois, United States: [www.osti.gov/servlets/purl/1184636](http://www.osti.gov/servlets/purl/1184636).

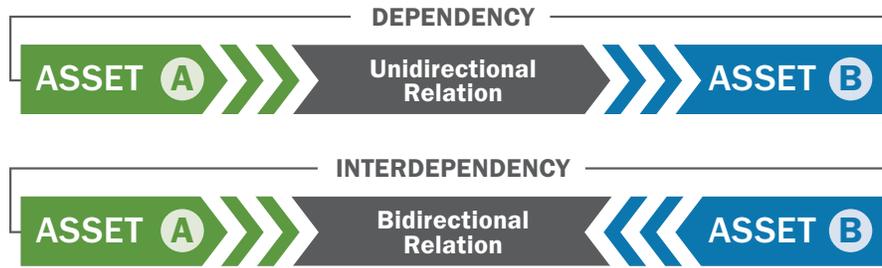


FIGURE 3.—Dependency and Interdependency between Two Assets.

Figure 4 provides a high-level illustration of common physical relationships among critical infrastructure systems. This matrix is a starting point to illustrate high-level dependencies across sectors that an incident may exacerbate; it is not a complete representation of all the relationships among sectors. In each column, red dots indicate that the supporting sector identified at the top of the column provides critical goods or services to the sector of interest along the left side of the matrix. In each row, red dots

indicate the supporting sectors that supply goods or services to the sector of interest. As figure 4 shows, five sectors provide goods or services to all other critical infrastructure sectors; their corresponding columns show a red dot for all critical infrastructure sectors. These sectors, which mostly encompass utility sectors, are identified in the NIPP as “lifeline” infrastructure sectors: communications, energy, IT, transportation systems, and water and wastewater systems.

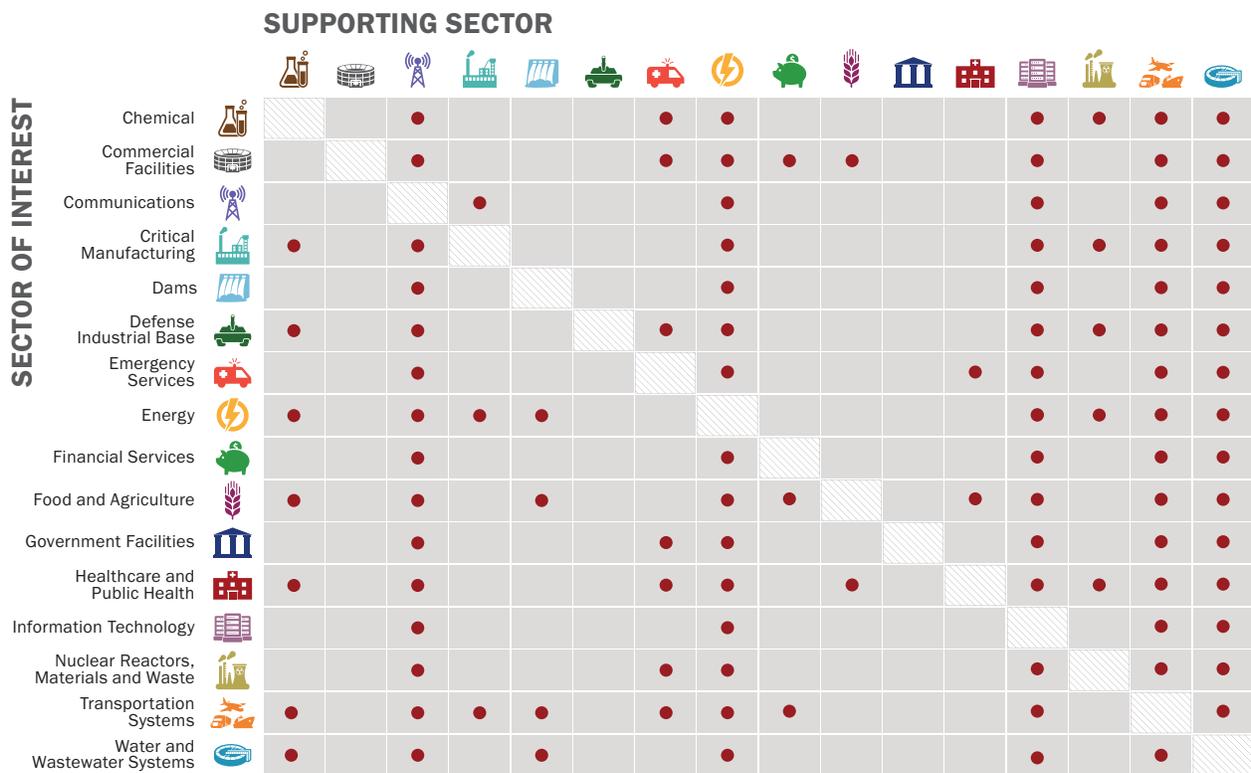


FIGURE 4.—Critical Infrastructure Dependency Matrix.

Another approach for characterizing infrastructure operations, their dependencies and interdependencies, and regional resilience is to focus on the functions performed by infrastructure systems rather than sector-specific labels. A functional construct—such as CISA’s taxonomy of National Critical Functions across four broad categories of connect, distribute, manage, and supply—allows analysts to consider how infrastructure enables a range of activities that are important to government, private sector, and community partners.<sup>11</sup> Example functions

include actions such as providing Internet-based content, information, and communication services; maintaining supply chains; managing wastewater; and generating electricity. Thinking about the functions of infrastructure allows for a different and more nuanced way of viewing how critical particular services are to individual entities, to regions, or to the nation as a whole. A functional approach also facilitates a more granular understanding of how infrastructure operations are interconnected.



## Evaluating Infrastructure Functions

In recent years, federal partners have released several complementary frameworks that embrace a functional approach to understanding infrastructure systems.

- **National Critical Functions:** CISA has identified a body of critical functions of government and the private sector that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety. These National Critical Functions provide a risk management lens that focuses less on a static, sector-specific or asset world view, and instead focuses on the functions an entity contributes to or enables. Information from CISA on National Critical Functions and their role in risk management is available at: <https://www.cisa.gov/national-critical-functions>
- **Community Lifelines:** The Federal Emergency Management Agency (FEMA) developed the community lifelines construct to support objectives-based response that prioritizes the rapid stabilization of key services after a disaster. Community lifelines include seven broad categories of the most fundamental services in the community that, when stabilized, enable all other aspects of society to function. Information on FEMA’s community lifelines construct is available at: <https://www.fema.gov/emergency-managers/practitioners/lifelines>
- **Community Resilience:** The National Institute of Standards and Technology (NIST) published guidance on community resilience planning to help communities meet essential needs, including but not limited to infrastructure systems and the built environment. Key to this process is understanding the functionality of critical infrastructure, which is a measure of how well a building or infrastructure system operates and delivers its service or meets its intended purpose. Information on the NIST community resilience planning process is available at: <https://www.nist.gov/topics/community-resilience/planning-guide>

<sup>11</sup> CISA, *National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience*. April 30, 2019. Accessed August 20, 2020. [www.cisa.gov/national-critical-functions](https://www.cisa.gov/national-critical-functions).

While security may be effective at addressing certain aspects of risk introduced by dependencies and interdependencies, security solutions alone are insufficient for addressing dependencies and interdependencies given their externality to the infrastructure system. For example, cybersecurity features for Internet-connected OT systems are an effective security approach for addressing the potential cyber threat to operations that are present due to dependence on external Internet service. However, these security solutions cannot address an outage of the Internet service provider itself. Entities can at least prepare for issues that they may not be able to secure themselves against; these actions embody features of resilience. Developing resilience is thus essential to managing the wide range of risks that dependencies and interdependencies present. Correspondingly, dependencies and interdependencies have a strong influence on the resilience of infrastructure, and the assessment of infrastructure resilience depends heavily on an understanding and evaluation of those dependent relationships and of the measures in place to mitigate the consequence of their potential disruption.

Dependencies and interdependencies can be risk multipliers for critical infrastructure. A threat or hazard can result in the loss of a service (e.g., electric outage), potentially impacting the critical infrastructure using this resource, which further affects other critical infrastructure dependent upon that infrastructure’s services. The total consequences of an event may be amplified by these connections (i.e., dependencies and interdependencies) that exist among critical infrastructure facilities.<sup>12</sup> Figure 5 illustrates the effect of critical infrastructure dependencies on risk.

Given the critical role of dependencies across all infrastructure operations, dependency analysis becomes a central capability in examining regional infrastructure resilience and security. The goal of dependency analysis is to develop knowledge of critical operational and spatial relationships among infrastructure by (a) identifying dependencies (upstream and/or downstream) that affect the operation of critical infrastructure, (b) examining the criticality of a dependency, the degree of coupling, and other key characteristics, like spatial and temporal aspects, (c) analyzing consequences of disruptions of one system on another/others, and (d) determining potential steps that can mitigate impacts and enhance resilience.

**EFFECTS OF INFRASTRUCTURE INTERDEPENDENCIES ON RISK**



FIGURE 5.—Potential Impacts from Critical Infrastructure Interdependencies on Risk Components.

<sup>12</sup> Petit, Frédéric, Duane Verner, David Brannegan, William Buehring, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Philips, and James Peerenboom. *Analysis of Critical Infrastructure Dependencies and Interdependencies (ANL/GSS-15/4)*. 2015. Retrieved from Argonne, Illinois, United States: <https://www.osti.gov/servlets/purl/1184636>.

## Connecting the Concepts of Risk, Preparedness, Security, Continuity, and Resilience

Given the growing focus on resilience, considering how it relates to other core concepts in homeland security, including risk, security, preparedness, and continuity is important.

- **Risk and Resilience:** Risk in the homeland security context is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood (a function of threats and vulnerabilities) and the associated consequences. Resilience is part of the risk equation in that it can influence an entity's vulnerability (or exposure) to different threats and hazards, as well as the consequences that might arise from an event. Ultimately, the process of analyzing risk is important because it shapes decision making on ways to manage risk by accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.<sup>13</sup> Thus, resilience is, fundamentally, part of an organization's broader risk management strategy. The goal of assessing system and asset properties—including threats, vulnerabilities, consequence, and resilience—is to enable decision makers to make informed choices that will result in cost-effective reductions in the risks associated with the range of threats and hazards entities face. Integrating resilience into planning and operations allows organizations to adapt to uncertainty and improve their ability to react to emerging threats and hazards. In fact, an inherent goal of resilience is being ready to adapt to both anticipated and unanticipated risks and remaining operational even in the uncertainty of dynamic environments.
  - **Preparedness and Resilience:** Preparedness involves planning, organizational, equipment, training, and exercise activities that build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from threats and hazards. Those five mission areas for national preparedness provide a simple way to organize risk management strategies. Prevention
- activities are most closely associated with efforts to address threats; protection efforts generally address vulnerabilities; response and recovery efforts help minimize consequences; and mitigation measures address the entire threat, vulnerability, and consequence spectrum. Infrastructure resilience measures fall into multiple preparedness mission areas—including protection, mitigation, response, and recovery—since resilience involves anticipating, resisting, absorbing, responding to, adapting to, and recovering from a disturbance. In many respects, preparedness and resilience are analogous: a very resilient infrastructure system will exhibit high levels of preparedness across all mission areas. This alignment between preparedness and resilience is evident in existing policy frameworks such as PPD-21, which explicitly states that making infrastructure more secure and resilient to all-hazards requires integration with the national preparedness system. Preparedness and resilience are attributes not just of the infrastructure itself, but of the organizations and workforces that operate these systems across multiple sectors.
- **Security and Resilience:** Infrastructure security is defined as reducing the risk to critical infrastructure by physical means or defensive cyber measures from intrusions, attacks, or the effects of natural or human-caused disasters. Securing critical infrastructure systems includes deterring, detecting, disrupting, or preparing for threats and hazards as well as reducing vulnerabilities. Infrastructure security actions typically center on prevention and protection efforts. Security contributes to the overall resilience of critical infrastructure, but is a single facet of a risk management strategy, primarily focused on threats and vulnerabilities. Resilience encompasses broader risk management and preparedness activities, and expands from threats and vulnerabilities to address consequences. Security is inherently focused internally within an organization: infrastructure operators can only effectively secure what they themselves own or manage. Resilience accounts for both internal and external factors, seeking to anticipate and prepare for events that security interventions

<sup>13</sup> DHS, *DHS Risk Lexicon: 2010 Edition*, September, 2010. Accessed February 13, 2020. <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

cannot prevent, such as a loss of power or communications service to a facility.

- **Continuity and Resilience:** Continuity planning for government and private sector partners centers on understanding how to maintain essential operations during an emergency situation. The goal of continuity planning is to reduce the consequences of any disruptive event to a manageable level;<sup>14</sup> this priority complements the core principles of resilience (i.e., preparing for and adapting to changing conditions as well as withstanding and recovering rapidly from disruptions). When continuity plans are activated, organizations expect to have limited resources and personnel available and anticipate not being able to perform all of their normal functions.<sup>15</sup> Resources and functions deemed essential in the continuity planning process are often interconnected across organizations; thus, the effectiveness of one organization's continuity plan can depend upon the successful execution of another organization's continuity plan. These interdependencies exist between government and private sector organizations; private sector may rely on certain government functions to stay open, just as government likely depends upon private sector resources for its own operations.<sup>16</sup> The more resilient an entity is, the better positioned it will be to weather challenges associated with emergency conditions and ensure that essential functions identified through continuity planning remain intact.

## Importance of Thinking Regionally

One of the chief challenges to infrastructure resilience is the increasing complexity of today's modern infrastructure. Infrastructure is connected to many other infrastructure assets, systems, and networks that they depend on for normal day-to-day operations, and these dependencies may span great distances.<sup>17</sup> These many points of connection and their geographic distribution make the infrastructure risk management environment much more complex, and demand a scale of engagement that exceeds single operators or governmental jurisdictions. Complex interdependencies crossing sectors and geographic regions pose coordination and cooperation problems that are not easily solved. These features of modern infrastructure operation necessitate a regional approach to assessing resilience that can accommodate both the geographic scale of infrastructure systems, their dependencies, and associated jurisdictional governance structures.

Businesses and communities increasingly use integrated physical and cyber systems to operate complex networks of interconnected infrastructures. As a result, an event occurring in one community or sector can cascade to other communities and sectors in ways that public and private partners may not fully anticipate. This is particularly true of disruptions in the lifeline sectors—energy, water and wastewater, communications, IT, and transportation systems—which provide services that are fundamental to most other infrastructure sectors. Faced with an increasingly unpredictable threat environment that includes cyber attacks, service disruptions from aging infrastructure, and highly disruptive weather events, critical infrastructure stakeholders understand that partnering to build resilience at the regional level is a key to achieving national resilience.<sup>18</sup>

<sup>14</sup> FEMA, *Continuity Guidance Circular*, February 2018, Accessed May 10, 2021. [www.fema.gov/emergency-managers/national-preparedness/continuity](http://www.fema.gov/emergency-managers/national-preparedness/continuity).

<sup>15</sup> Ibid.

<sup>16</sup> Ibid.

<sup>17</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>18</sup> NIAC, *Strengthening Regional Resilience: Final Report and Recommendations*. November 21, 2013. Accessed February 13, 2020. [www.cisa.gov/niac-reports-and-recommendations](http://www.cisa.gov/niac-reports-and-recommendations).

Often, critical infrastructure systems that are essential to one community also support multiple other jurisdictions. To meaningfully understand the resilience of infrastructure systems, the geographic aperture of the assessment may need to extend well beyond the geographic boundaries of an individual community. Regions are more flexible constructs for analysis that can expand or contract based on evolving threat and hazard patterns, the geographic extent of an infrastructure system, and infrastructure dependencies and interdependencies. A region can include a single community or multiple communities; it can transcend state boundaries to address select communities from multiple states or even multiple states in their entirety. Using more flexible regional constructs in infrastructure resilience analysis allows participants to best align the boundaries of their assessment efforts to the questions they want to explore rather than being locked strictly into existing geopolitical footprints.

A valuable element of regional assessments of critical infrastructure resilience is that these analyses can help bridge the gap between *communities* that have established geographical boundaries and governance structures and *regions* that reflect service areas of infrastructure, hazard exposure, and environmental factors that cut across one or more communities. Regional resilience analysis—and the potential actions to strengthen resilience that arise from it—can help communities work together to address broader resilience challenges that are too large to manage on their own. Fundamentally, regions represent an intermediate stage between local and national concerns. Defining and using regional constructs in infrastructure resilience analysis allows practitioners to find a middle ground that meets the need of state, local, tribal, and territorial partners; infrastructure owners and operators that have geographically distributed service areas; and federal entities focused on critical infrastructure of national significance.



## Defining a Region

In the context of infrastructure resilience assessments, region is a flexible term intended to help define the geographical footprint for an effort that stretches beyond a single location. Depending on resilience issues being explored and the partners interested in participating, a regional assessment could explore any of the following types of regions:

- Political boundaries (e.g., cities, counties, states, countries)
- Geographic extent of large infrastructure systems (e.g., electric grid; pipelines; water and wastewater systems; transportation networks; food production, processing and distribution)
- Natural features that connect communities (e.g., navigable waterways, watersheds)
- High-density clusters of key industries and commercial activity
- Risk exposure zones (e.g., seismic zone, floodplains, hurricanes/tropical storm paths)

Regional assessments can characterize the role of local and regional infrastructure systems in broader national infrastructure systems or nationally significant supply chains. Furthermore, regional assessments can help identify the dynamics (i.e., dependencies and interdependencies) between national-scale infrastructure and smaller infrastructure systems. For example, the disruption of a small port that serves as the primary point of import for a chemical feedstock necessary for petroleum processing could cause national disruptions. Resilience at a community or regional level involves dimensions of resilience beyond critical infrastructure, including supply chains, governance, and civil society issues that can be hard to quantify. Identifying the critical linkages between local and national infrastructure allows

for prioritization of local, state, and national resources to improve the resilience of these links. These improvements can generate significant return on investment as they provide different benefits at the local, regional and national levels.



### Defining the Value Proposition

The value proposition for assessing infrastructure resilience at a regional level centers on the following:

- Understanding how infrastructure systems in a region function and their associated dependencies and interdependencies;
- Incentivizing greater coordination among public and private sectors and different levels of government;
- Defining shared resilience objectives for regional partners and leveraging collective resources effectively to achieve them;
- Informing design decisions, capital investments, and mitigation measures in infrastructure systems that enhance resilience; and;
- Planning jointly to respond to and recover from various threats and hazards.

## Challenges in Strengthening Regional Resilience

Efforts to understand, assess and strengthen infrastructure resilience at a regional level face a diverse range of significant challenges. Some of the driving attributes that create these challenges include the following: geographically distributed, yet highly interconnected infrastructure operations; growing technological complexity; prevailing business practices; business climate, legal and regulatory realities; differing organizational mindsets; and an expanding risk environment. These and other considerations create fundamental but not insurmountable challenges associated with assessing and ultimately strengthening regional infrastructure resilience. Identifying such challenges up front can help decision makers and analysts approach regional assessments from a more realistic context and help to better define solutions and strategies.

■ **Geographic reach:** individual infrastructure facilities and systems can be found in discrete geographic locations, but the information, products, services, and functions that they produce and rely upon can flow across jurisdictions, regions, and even international borders. Utilities such as electric power and natural gas providers often have systems that span numerous regions or states. Manufacturers increasingly rely on national and global level product sourcing and sales, requiring greater reliance on extended transportation links. They also face greater risk from factors over which they have less control. These geographically distributed operations require increased levels of coordination within and across companies and organizations, as well as exposure to additional layers of risk. In addition, large-scale disasters that can span multiple jurisdictions introduce the need for joint governmental coordination and action for effective response and recovery. In short, infrastructure resilience cannot be addressed in a single geographic setting, but instead must contend with an increasingly diverse geographic landscape with the need to work with numerous different governmental jurisdictions.

- **Increased interconnectedness:** the degree to which infrastructure facilities and systems are dependent on one another—the strength or “tightness” of operational coupling—continues to increase.<sup>19</sup> Tight coupling between infrastructures is not a new phenomenon; however, many of these classic dependencies are largely unidirectional. For example, water pumps have always needed electricity to pump water to higher elevation, but the loss of water pump pressure is unlikely to affect electricity production or transmission. Infrastructure is becoming more tightly coupled to other infrastructure and, at the same time, more interactively complex. This means that the potential for cascading effects across companies, sectors, and regions is also increasing. Complex interdependencies crossing sectors and geographic regions pose coordination and cooperation challenges that are not easily solved. This affects both the ability to analyze and manage risks, and respond to emergencies and other disruptions. Risks and vulnerabilities that arise from dependencies between sectors and organizations, and that do not “belong” to any single actor, are far more difficult to assess and to prepare for.<sup>20</sup>
- **Penetration of advanced technologies into infrastructure operations:** over the last two decades, billions of people and things—including personal computers, mobile devices, wearable devices, home appliances, and sensors—have been connecting to networks and to each other. Electronics have become less expensive, more compact, and better performing. Connections between an increasing number of devices have been supported by improving wireless technologies (e.g., 4G and 5G), Internet Protocol

version 6, and other developments that increase the speed, availability, and bandwidth of network connections.<sup>21</sup> The pace of technology innovation is driving significant changes in the information and communications technology ecosystem that underpins infrastructure systems writ large. Notable trends impacting infrastructure systems include the following: increasing adoption of cloud computing by enterprises and consumers; growing focus on interoperability; explosive growth in mobile computing and mobile applications; expanding deployment of the Internet of Things and the trend in smart sensors/smart devices controlling physical systems; and constantly increasing IT operational complexity.<sup>22</sup> Although this increasing availability of data and information used to monitor, operate and maintain critical infrastructure enables more efficient and effective practices, it is also vulnerable to unauthorized access that could affect its confidentiality, integrity, or availability.<sup>23</sup>

- **Prevailing business practices:** today’s economy puts a premium on speed and reactivity, with growing trends in lean manufacturing and just-in-time inventory management. Businesses focus intently on improving efficiency and decreasing waste, leading to production cycles that react to demand signals from consumers and seek to maximize flexibility. Nimble business practices can help manufacturers, suppliers, and consumers adapt to changing conditions, but they can also increase infrastructure dependencies and complicate risk management, introducing new vulnerabilities and potentially limiting resilience capacity.

<sup>19</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>20</sup> Almklov, Petter, Stian Antonsen, and Jørn Fernstad, “Organizational Challenges Regarding Risk Management in Critical Infrastructures,” *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis* (London: Springer, 2015).

<sup>21</sup> NNSTAC (National Security Telecommunications Advisory Committee), National Security Telecommunications Advisory Committee, Report to the President on Emerging Technologies Strategic Vision. July 14, 2017. Accessed December 17, 2020. [www.cisa.gov/publication/2017-nstac-publications](http://www.cisa.gov/publication/2017-nstac-publications).

<sup>22</sup> CISA, *Information Technology Sector Specific Plan*. 2015. Accessed February 13, 2020. [www.cisa.gov/2015-sector-specific-plans](http://www.cisa.gov/2015-sector-specific-plans).

<sup>23</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

Furthermore, critical infrastructure ownership and operations are often distributed.<sup>24</sup> Networks of private and public entities, rather than single companies, run today’s infrastructure. This practice has transformed some infrastructure industries from integrated companies into “single-purpose organizations,” with specialized roles and functions that do not overlap. This trend has increased the number of organizations that need to be involved to identify, analyze, and effectively manage infrastructure risks that cross organizational boundaries.<sup>25</sup>

At the same time, however, the challenges of increasingly complex and interdependent infrastructure converge with the large number of distributed actors involved in supporting operations to create a lack of transparency. This is a logical result of some core environmental factors: a competitive business environment where protecting proprietary information and gaining competitive advantage are keys to success; information security concerns; and limited resources to collect, manage, analyze, and act on that type of information. Nevertheless, critical infrastructure partners need timely, reliable, and actionable information regarding threats, vulnerabilities, and consequences from across their operational landscape to manage risk effectively, and this will require greater coordination and planning among business partners. Ongoing policy processes continue to focus on reducing technological and regulatory constraints that can hamper data sharing across infrastructure partners.

- **Legal and regulatory realities:** the operation of any infrastructure facility or system must comply with an array of government laws, regulations, guidelines, and policies. This is also the case with the manufacture, distribution, transportation and use of many products required to operate infrastructure. For example, an industrial factory must abide by a wide range of safety, environmental and other rules, but likely also faces regulations affecting how incoming raw materials can be transported

and handled, how much of certain materials can be held onsite, how many hours per day their drivers can operate, and a wide array of other restrictions. This legal and regulatory landscape can become particularly important at times of stress within infrastructure operations, including large-scale disasters, when maximum operational flexibility may be needed to maintain or rapidly reconstitute business operations. Mechanisms to temporarily alleviate or waive such regulatory constraints under certain circumstances exist, but conditions and processes necessary for doing so often are not widely known.

- **Organizational goals and constraints:** another challenge in assessing and strengthening regional infrastructure resilience is the need to consider diverse organizational goals and constraints within public and private sectors. For example, industry focuses on business performance, customer satisfaction, reputation, and profitability, while government focuses on community priorities and legal enforcement. Their tolerance for risk varies within and across public and private partners, as do resources available to manage that risk. Reconciling these pressures can require significant coordination and action, especially when it comes to complex, fast-moving, and potentially life-threatening disasters. More broadly, public and private partners alike may face challenges in perceiving, accounting for, planning against, and resourcing for low-probability, high-consequence events. These large-scale disasters may be viewed as simply too overwhelming to ponder, which can hinder organizational commitment to plan and resource accordingly. Ultimately, the value proposition of and business case for infrastructure resilience may not always be clear to both industry and government partners, particularly when faced with allocating limited resources across a lengthy list of priorities. Though each has a different perspective on risk management and the value proposition of resilience, fortunately, government and industry have a natural and compelling shared interest in working together to ensure

<sup>24</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>25</sup> Almklov, Petter, Stian Antonsen, and Jørn Fernstad, “Organizational Challenges Regarding Risk Management in Critical Infrastructures,” *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis* (London: Springer, 2015).

the security and resilience of infrastructure.<sup>26</sup> System-of-systems mechanisms (e.g., using scenarios to frame common concerns) can help focus critical infrastructure partners on issues that supporting the region.

- **Expanding risk environment:** the overall risk environment for critical infrastructure is complex, expanding, dynamic, and uncertain. Geographically stretched operations and supply chains increase risk exposure for businesses; greater connectedness and business relations can lead to secondary vulnerabilities derived from external partners; and full-scale reliance on information technologies, automation, and related capabilities introduce entirely new sets of threats and embedded vulnerabilities. Direct risks are also growing in many respects. Some of the factors that shape the growing diversity and scale of risks facing critical infrastructure operations include: more extreme and more frequent destructive weather events; aging infrastructure systems and components; greater reliance and stresses upon infrastructure systems; increasing frequency and severity of cyber attacks; increasing density of populations and business operations; heightened threat from terrorism and violent crime; ongoing use of hybrid tactics by nation-state adversaries; and the growing incidence of epidemics, novel disease outbreaks, and other public-health crises domestically and globally.<sup>27,28</sup>

(For example, see the callout box on page 22 for a discussion of the coronavirus pandemic and infrastructure resilience.) These risks introduce challenges for physical infrastructure, related cyber systems, and the personnel who operate them.

These and other challenges can create a difficult landscape on which to assess and strengthen regional infrastructure resilience. Yet they must be recognized, accounted for, and integrated into resilience assessments and planning in order to achieve progress.

The foundational concepts presented above related to regional infrastructure resilience and the corresponding need for frequent assessment and analysis provide a foundation for organizing executable strategies and plans. Thinking about and examining diverse, interconnected, and critical infrastructure systems that span large geographic areas should always take full account of these concepts. Analysts and decision makers run the risk of ineffectual or even counterproductive analysis if these concepts are not properly integrated. Once this theoretical basis is established, the tangible value of regional infrastructure resilience can be pursued through concrete, real-world assessments and analysis that lead to new knowledge and action. Turning this theory into practice through a repeatable process is the focus of part 2 of this document.

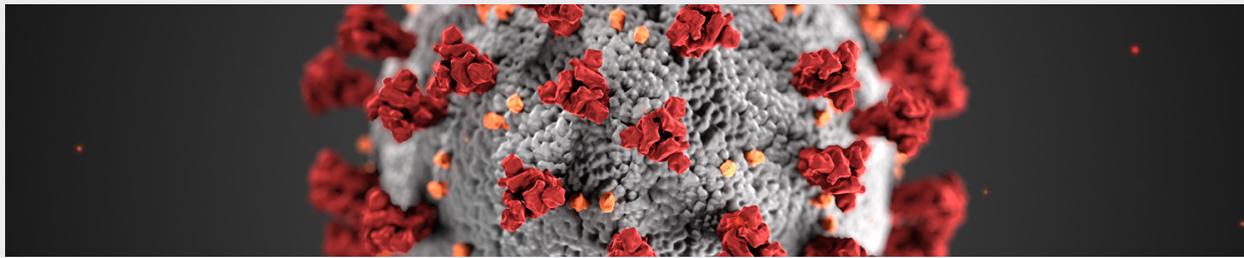


<sup>26</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>27</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

<sup>28</sup> CISA, *Strategic Intent: Defend Today, Secure Tomorrow*. August, 2019. Accessed February 13, 2020. [www.cisa.gov/publication/strategic-intent](http://www.cisa.gov/publication/strategic-intent).

# INFRASTRUCTURE RESILIENCE ASSESSMENT AND THE CORONAVIRUS PANDEMIC



In 2020, the national response to the COVID-19 outbreak surfaced a set of complex and novel factors related to critical infrastructure resilience and new avenues to explore in regional assessment efforts. Overarching effects of the pandemic on critical infrastructure owners and operators included:

- Shortages in personnel needed to maintain infrastructure operations, occurring due to illnesses, social distancing policies, transportation system constraints, or limited supplies of personal protective equipment
- Disruptions to global supply chains that underpin critical infrastructure operations in some sectors
- Changes to typical supply and demand patterns of key commodities and infrastructure systems
- Rapid and extensive transition to telework

The disease progression and the public health response to it affected critical infrastructure in ways that differed from historical experiences. First, the actual effects experienced by critical systems generally were not related to physical damage to the infrastructure itself. In events such as hurricanes, earthquakes, and floods, the physical hardware is often damaged or destroyed, degrading operations and putting a premium on rapid repair and restoration. The challenges experienced by infrastructure systems during the COVID-19 response were rooted more in personnel availability and supply-demand disconnects. Second, the geographic scope of the disruptive effects on infrastructure was significantly larger than a typical disaster. Instead of the local or regional consequences typically experienced, COVID-19 affected communities and infrastructure

simultaneously not only in the United States but across the globe. Third, while lifeline infrastructure sectors—including energy, water and wastewater, transportation, communications, and IT—were directly impacted by the pandemic, other infrastructure systems (e.g., healthcare and public health, food and agriculture) were also at the center of the national response.

During this time, CISA worked with government partners and the private sector to develop an advisory list that characterized the essential critical infrastructure workforce. The list was intended to help state, local, tribal, and territorial officials and organizations protect their workers and communities, while also ensuring the continuity of critical functions. The advisory list identified workers who conduct a range of operations and services that are typically essential to continued viability of critical infrastructure. This characterization of an essential workforce can be a useful resource in regional infrastructure resilience assessments, particularly in evaluating dependencies within and across sectors.

Some of these experiences will likely have lasting effects on how infrastructure functions and on the planning and design of infrastructure to support changing urban spaces. The long-term impacts of the COVID-19 experience on urban design, transit networks, telework patterns, communications/IT networks, and aging public infrastructure remain unsettled, but operations are unlikely to return to exact pre-COVID conditions. Therefore, future assessments of regional infrastructure resilience will need to begin to account for these emerging dynamics and adapt to new trends emerging in infrastructure planning, design, and operations.



## PART 2

# METHODOLOGY FOR ASSESSING REGIONAL INFRASTRUCTURE RESILIENCE

25	Engage Partners
28	<b>Step 1:</b> Identify Problem
32	<b>Step 2:</b> Design Assessment
41	<b>Step 3:</b> Collect Data
56	<b>Step 4:</b> Analyze
88	<b>Step 5:</b> Document and Deliver Results
94	<b>Step 6:</b> Promote Action
100	Tying it All Together
112	Conclusion

## PART 2

# METHODOLOGY FOR ASSESSING REGIONAL INFRASTRUCTURE RESILIENCE

This section provides guidance on a generalizable, scalable methodology for assessing the resilience of critical infrastructure at a regional level, reflecting lessons learned from 100 projects implemented across the country on dozens of infrastructure systems through the RRAP since 2009. Key processes and analytical techniques are described that should result in actionable options that stakeholders can adapt to their own needs for enhancing resilience.

The process begins with identifying a problem, and continues through assessment design, data collection, analysis, documenting and delivering results, and promoting action by stakeholders to improve resilience. All steps require partner engagement, whether to identify shared challenges, achieve buy-in on the effort, solicit data, share preliminary analytical findings, or support specific follow-on recommendations arising from the assessment. The overall process is shown in figure 6, followed by a brief explanation of what is addressed at each step, recognizing that some activities in different phases may be able to run concurrently. The remainder of this chapter provides a deeper examination of what each step entails.



FIGURE 6.—General Steps in Assessing Regional Infrastructure Resilience.

- 1. Identify Problem:** while the idea for a resilience assessment can originate from a variety of sources, this important first step begins with identifying a problem that regional partners need to address and developing a concept that they can execute together.
- 2. Design Assessment:** this step involves defining the key research questions that regional assessment efforts will attempt to address, establishing the geographic extent of the effort, identifying infrastructure systems to be considered in the assessment, and articulating the specific steps that stakeholders will take to address key research questions.
- 3. Collect Data:** activities can include open-source research, multi-agency collaboration, subject matter expert interviews, facilitated discussions, site assessments, and other steps that help stakeholders capture information needed to address the assessment's key research questions.
- 4. Analyze:** this step involves the application of an analytical approach that incorporates one or more analytical techniques (e.g., geospatial analysis, modeling and simulation) to evaluate the infrastructure systems of interest.
- 5. Document and Deliver Results:** this step centers on documenting specific issues, challenges, and opportunities discovered through the assessment and defining potential courses of action that can begin to address identified resilience gaps.
- 6. Promote Action:** the final step involves laying the groundwork for action on analytical findings and taking tangible steps to enhance resilience through capital investments, planning efforts, training, and exercises.

## Engage Partners

Successful regional infrastructure assessments build in opportunities for continuous partner engagement throughout the effort, starting with scoping and continuing all the way through the delivery of results with an eye toward long-term implementation of resilience enhancement measures. A collaborative risk management strategy that is jointly developed through a public-private partnership elevates the effectiveness of efforts to secure critical infrastructure and enhance its resilience.<sup>29</sup> Building voluntary coalitions and other types of public-private partnerships creates a strong value proposition in which partners recognize distinct benefits from participation that strengthens resilience by building a strong track record of success.



### Working With Tribal Partners

The U.S. Government has a unique legal and political relationship with American Indian and Alaska Native Tribal Governments. The United States recognizes the right of federally recognized Indian Tribes to self-government. As of March 2020, 574 federally recognized tribes existed. In addition, some tribes are recognized by states. State-recognized Indian tribes are not necessarily federally recognized, but federally recognized tribes may also be state-recognized. These categories are useful to identify resources that tribal partners can access. A list of federally recognized tribes is available through the U.S. Bureau of Indian Affairs at [www.bia.gov/tribal-leaders-directory](http://www.bia.gov/tribal-leaders-directory). Information about federally and state-recognized tribes is available from the National Conference of State Legislatures at [www.ncsl.org/research/state-tribal-institute/list-of-federal-and-state-recognized-tribes.aspx](http://www.ncsl.org/research/state-tribal-institute/list-of-federal-and-state-recognized-tribes.aspx).



### Balancing Voluntary and Regulatory Processes

In a voluntary assessment, partners are not compelled through regulation to participate but rather do so because they see value in coming to the table voluntarily. In other cases, regulation may require owners and operators of infrastructure systems to share information or participate in assessments. Understanding this landscape is an important step in scoping a regional assessment. Private sector partners may hesitate to join in a voluntary assessment if the infrastructure in question is already subject to regulation; doing so may lead to duplicate work of potentially limited value. In addition, if state, local, tribal, or territorial regulators are identified as end-recipients of a voluntary assessment, private sector partners may hedge on participating and sharing potentially sensitive information with that community. However, regulatory bodies can be valuable resources for assessment teams in understanding how particular industries operate and in accessing relevant data sources collected through established processes.

Establishing and maintaining strong partnerships with federal, state, local, tribal, and territorial government officials and private-sector organizations across multiple disciplines is essential for conducting a successful resilience assessment. It is particularly important to include and obtain buy-in from the relevant infrastructure owners and operators (often both private and public sector), whose facilities and systems are typically at the core of any initiative to enhance regional infrastructure security and resilience. Representation from multiple industries can help ensure that cross-sector issues are identified and factored into the assessment.

<sup>29</sup> CISA, *Fact Sheet on the National Risk Management Center*. November, 2018. Accessed February 13, 2020. [www.cisa.gov/publication/national-risk-management-center-fact-sheet](http://www.cisa.gov/publication/national-risk-management-center-fact-sheet).

Regional infrastructure assessments can vary in scope and scale, but often the participation of a wide variety of stakeholders is necessary to achieve success, including private-sector facility owners and operators, industry organizations, emergency response and recovery organizations, utility providers and regulatory authorities, transportation agencies and authorities, planning commissions, law enforcement and security organizations, academic institutions, and research centers. On the local level, government, business, and civic organizations have unique knowledge of, access to, and communication with potential partners throughout the community.<sup>30</sup> Figure 7 provides examples of potential assessment participants from across government, private sector, and academic communities.

Partnership is essential to effective efforts to understand and strengthen resilience in a region. Each step in a resilience assessment requires engagement with a variety of stakeholders to some degree. Whether seeking input on common resilience challenges facing the region, developing a specific and viable concept for an assessment, vetting preliminary analysis, or even just hosting regular meetings to discuss progress, the role of partners in regional resilience assessments is ever-present. Moreover, taking action to address regional resilience gaps identified during the assessment likely requires coordination among numerous stakeholders hailing from multiple organizations and jurisdictions. Table 2 provides examples of how partners should be engaged throughout the regional infrastructure resilience assessment process.

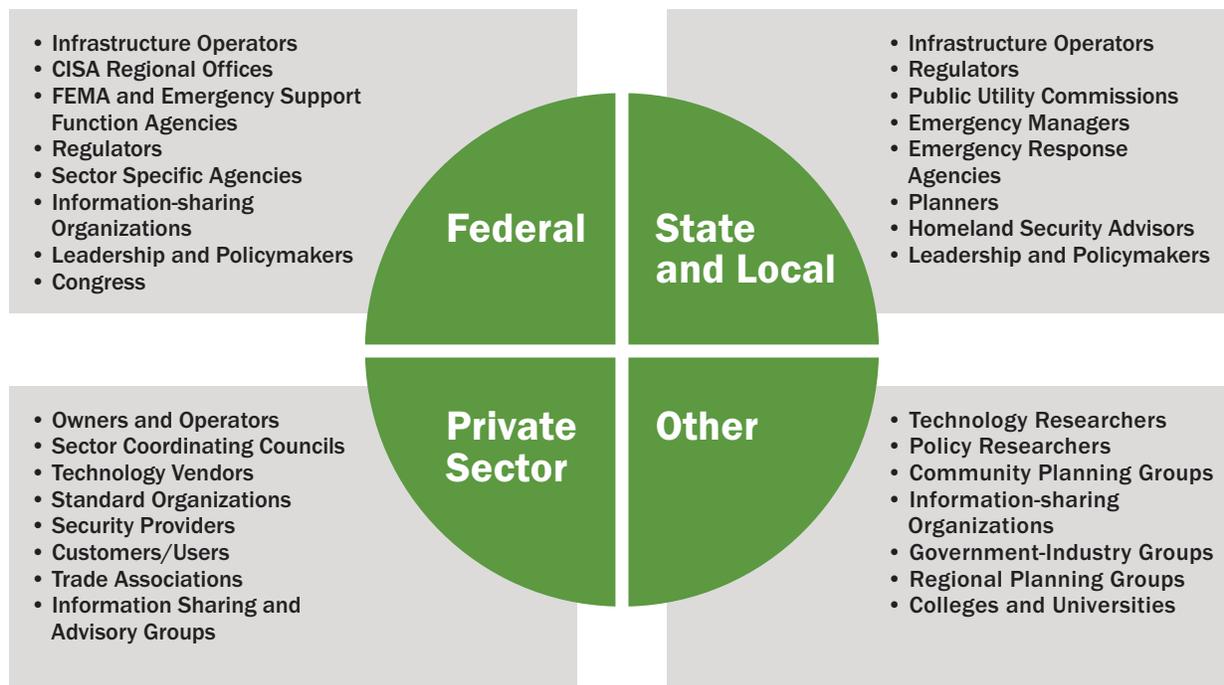


FIGURE 7.—Example Partners for Regional Infrastructure Resilience Assessment.

<sup>30</sup> National Research Council, *Building Community Disaster Resilience Through Private-Public Collaboration* (Washington, DC: The National Academies Press, 2011).

**TABLE 2**

## Opportunities for Partner Engagement in Regional Infrastructure Resilience Assessments

Phase of Assessment	Opportunities for Partner Engagement
<b>Identify Problem</b>	<ul style="list-style-type: none"> <li>Discussions with existing working groups, centered on infrastructure resilience challenges identified by these organizations</li> <li>Real-world incident after-action reviews</li> <li>Improvement actions from tabletop and functional exercises</li> </ul>
<b>Design Assessment</b>	<ul style="list-style-type: none"> <li>Scoping meetings</li> <li>General information-sharing conference calls</li> <li>Regular status meetings and in-progress reviews</li> </ul>
<b>Collect Data</b>	<ul style="list-style-type: none"> <li>Interviews</li> <li>Facilitated discussions</li> <li>Infrastructure facility visits</li> <li>Engagements about data sharing and protection</li> </ul>
<b>Analyze</b>	<ul style="list-style-type: none"> <li>Discussions to inform analysis assumptions and refine analytic approaches</li> <li>Meetings to review and validate findings</li> </ul>
<b>Document and Deliver Results</b>	<ul style="list-style-type: none"> <li>Stakeholder reviews of draft outputs</li> <li>Outbriefs with team members, key stakeholders, and leadership to share results</li> </ul>
<b>Promote Action</b>	<ul style="list-style-type: none"> <li>Follow-ups to scope next steps and implementation priorities</li> <li>Supplemental engagements to facilitate understanding and application of results</li> <li>Participation in periodic leadership and working-level meetings to address assessment findings and track progress</li> </ul>



### Developing Broad-based Partnerships

While a strong partner-base from across the public and private sector is typically essential to an assessment, obtaining this requirement can be a significant challenge. Depending on the topic, input from dozens of distinct organizations may be needed for a successful assessment. Furthermore, the fact that a given topic is seen as ripe for an assessment may indicate that crucial partnerships may need strengthening. The RRAP often benefits from the nationwide presence of DHS and associated networks of partners, but more localized assessments may face challenges in identifying and convincing certain key partners to participate. This is not always the case, but can be a factor in devising a successful assessment.

# STEP 1 IDENTIFY PROBLEM



To various degrees, communities across the country face a common set of gaps in understanding and addressing infrastructure resilience. As these gaps are identified, regional partners can use them to form the basis of potential assessments. A sound concept for an assessment starts with an explicit question or a problem in need of solving. Some assessment concepts begin with a challenge or knowledge gap that has been identified by one or more stakeholders based on real-world experience or previous research. For example, a state emergency manager might not understand how a critical infrastructure system in their jurisdiction operates or what vulnerabilities or dependencies it has. In other instances, communities may proactively seek to understand how infrastructure resilience gaps observed elsewhere might apply to them before they experience a major infrastructure-related disruption. Because resilience-related projects essentially function as a way to address knowledge gaps, when a partner presents a problem as an idea for an assessment, key follow-on questions to consider include what knowledge is missing that would help resolve this problem and what research would help generate this information.

## Potential Sources for Regional Assessment Concepts

A successful assessment—one that has diverse partners actively involved and yields actionable results for strengthening resilience—will often be anchored in or driven by broader ongoing efforts. Viable concepts for an assessment identified by regional partners may have an air of familiarity to them, as they could be issues that have arisen before on multiple occasions, surface regularly during exercises, or relate to ongoing preparedness, mitigation, response, or recovery initiatives. They should reflect some degree of foundational research by core stakeholders to confirm the need for an assessment and the viability of any early proposed concepts. Reviewing a range of inputs for potential assessment concepts can foster a common understanding of challenges facing public and private infrastructure partners and facilitate the identification of root causes to address through the assessment.



### Identifying Assessment Concepts

The genesis for an assessment may come from an informal conversation with a private sector stakeholder who believes they are unable to influence collaboration within an industry that is highly regulated and competitive. Assessments led by an organization outside the regulated/competitive industry often highlight the benefits of inter-industry and industry-government cooperation in a forum that is neutral. By identifying opportunities for the industry to address shared risks and working with regional public safety and emergency management officials, resilience challenges are highlighted as much more than an individual organization’s issue.

## Past experience with real-world incidents

Past experience with disruptions in infrastructure systems arising from real-world incidents (e.g., hurricane, wildfire, winter storm, cyber attack) is a compelling source for resilience assessment concepts. After-action reports document strengths and areas for improvement identified during response and recovery efforts and shed light on challenges that emerged in an actual event. These findings are valuable not only for the communities where the event occurred but for other regions and entities across the country who can benefit from resilience challenges identified and lessons learned elsewhere and incorporate them into their own risk management processes.



### Identifying Assessment Needs

Examples of multi-organizational groups that focus on infrastructure topics and could inform the development of a regional infrastructure assessment include the following:

- Area Maritime Security Committees
- FEMA Regional Interagency Steering Committees
- InfraGard chapters
- Business Executives for National Security chapters
- Councils of Governments
- Regional consortiums (e.g., All Hazards Consortium, ChicagoFIRST, Pacific Northwest Economic Region)

## Working groups and partnership organizations

Numerous working groups and partnership organizations exist nationwide, designed to facilitate information sharing and identify shared priorities. Strong partnerships with federal, state,

local, tribal, and territorial government officials and private sector organizations across multiple disciplines are essential to successful resilience assessments. However, they also provide established bodies that can identify resilience gaps, vet potential regional assessments to explore those gaps, advocate for collaborative approaches, and ultimately implement recommendations for resilience enhancement that arise from the analysis. Existing working groups may include stakeholders from a variety of organizations including the following:

- Private sector facility owners and operators
- Emergency response and recovery organizations
- Utility providers and regulatory authorities
- Transportation agencies and authorities
- Metropolitan planning organizations
- Law enforcement and security organizations
- Tribal councils
- Academic institutions and research centers
- Industry associations

## Prior assessments, operational plans, and exercises

Existing facility-specific reports, such as voluntary facility vulnerability assessments, may highlight the impact that individual facilities can have on the resilience of infrastructure in a region, which can translate into a good starting point for an assessment concept. In particular, assessments conducted at facilities located within the geographical focus area or supporting infrastructure that have the potential to provide resilience information may be helpful. Operational plans also provide a potential source for consideration. The collaborative planning process used to develop emergency operations plans and their supporting annexes can surface knowledge gaps that form the basis of a regional infrastructure resilience assessment. For example, a regional disaster plan focused on responding to a long-term power outage could provide the impetus for an assessment of how a significant disruption to electric power would affect other infrastructure sectors in the region. Alternatively, a regional catastrophic response plan focused on the aftermath of a major earthquake could lead to an assessment of the resilience of

highway transportation networks and their role in facilitating the delivery of supplies post-earthquake to affected areas. Similarly, lessons learned from tabletop and full-scale exercises may also identify regional resilience gaps that merit further exploration. Previous community or regional projects may also provide ideas, as well as open-source studies.

## State and local hazard analyses and capabilities assessments

FEMA requires states and major urban areas to complete hazard analyses and capabilities assessments in order to understand what capabilities are needed to effectively manage their risks. Communities complete the Threat and Hazard Identification and Risk Assessment (THIRA) process every three years, exploring what threats and hazards might affect them, what the potential impacts would be, and what capabilities should be in place to manage that risk. The THIRA helps communities understand their risks and what level of capability they need to address them. The Stakeholder Preparedness Report (SPR) is an annual self-assessment process which allows states and urban areas to measure the capabilities they currently have in place, what gaps exist, and what steps are needed to close those gaps or sustain existing capabilities. Together, the THIRA and SPR provide a high-level snapshot of regional risk and the capability gaps needing attention by state and local partners.<sup>31</sup> A number of states may use the THIRA and SPR processes to determine strategic goals and objectives and identify key agencies that are important for collaboration and engagement. Some states use the THIRA and SPR outputs to prioritize how they use preparedness grant funding from FEMA (e.g., Homeland Security Grant Program). With some additional shaping, an identified hazard and observed capability gaps can translate into a critical infrastructure resilience question worthy of examination and assessment.

In addition to the THIRA and SPR, emergency management programs engage continuously in mitigation planning, which involves identifying risks and vulnerabilities associated with natural disasters, and developing long-term strategies for protecting people and property from future

hazard events. Mitigation plans are key to breaking the cycle of disaster damage, reconstruction, and repeated damage. A core component of the mitigation planning process is an assessment of risk for the relevant jurisdiction that is current and reflects new hazard data (e.g., recent events, current probability data, loss estimation models, flood studies, and consideration of changing environmental or climate conditions that may affect and influence long-term vulnerability). Risk considerations and related priorities from mitigation plans can inform concepts for regional resilience assessments.

## Threat identification by public and private partners

Beyond the THIRA and mitigation planning processes, additional information sharing and analysis mechanisms exist for identifying potential threats that may be relevant to one or more infrastructure sectors and point to potential knowledge gaps that an assessment could explore. For example, fusion centers operate as focal points for states and major urban areas for receiving, gathering, analyzing, and sharing threat-related information between federal, state, local, tribal, territorial, and private sector partners. Fusion centers engage law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection and private sector security personnel in gathering and sharing threat-related information. Fusion centers conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Another source of threat-related information is information sharing and analysis centers (ISACs), which support efforts by owners and operators of critical infrastructure to protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. Nearly two dozen ISACs representing infrastructure sectors and subsectors collect, analyze, and disseminate threat information to members and provide them with tools to manage risks and strengthen resilience. Inputs from these types of entities can inform the identification of potential topics for evaluation through infrastructure resilience assessments.

<sup>31</sup> FEMA, *Comprehensive Preparedness Guide (CPG) 201, 3rd Edition, Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*. May 2018. Accessed February 13, 2020. [www.fema.gov/emergency-managers/risk-management/risk-capability-assessment](http://www.fema.gov/emergency-managers/risk-management/risk-capability-assessment).

## National strategic priorities for risk management and infrastructure resilience

CISA leads a national effort to defend critical infrastructure against current threats, while working with partners across all levels of government and in the private sector to secure against evolving future risks. With respect to infrastructure resilience, CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.<sup>32</sup> National Critical Functions, strategic plans, technical reports, and policy papers from CISA and other federal partners shed light on issues of national concern that may influence regional priorities, suggest viable opportunities for partnership, and provide a framework for assessment and analysis.

## Pre-existing awareness of shortcomings in infrastructure knowledge and resilience

Often, assessment concepts arise organically based on pre-existing awareness that gaps exist in how a community or region understands or is positioned to address a significant infrastructure resilience challenge. These knowledge gaps may have been known for years or may be new issues arising from the evolution or expansion of critical infrastructure systems and the communities they support. These types of assessment concepts may present themselves in this type of statement: *“We know that industry X is vital to our regional economy, but we are concerned that we do not*

*know enough about how this industry operates to be sufficiently prepared for its stabilization and recovery following a major disaster.”* These organic questions and concepts often need additional refinement but frequently lead to some of the most relevant and valuable analysis for a given region.

## Obtaining Buy-in

Achieving buy-in from key stakeholders who own relevant infrastructure is critical to increasing the willingness of stakeholders to share data and the likelihood of taking action based upon the results of the resilience assessment. Obtaining this buy-in from private sector infrastructure owners may be challenging due to concerns about potential future regulation, business sensitivities, or competing viewpoints of key partners. Identifying and effectively communicating the explicit, partner-specific benefits of participation in regional resilience assessments can help assuage concerns about perceived risks of support. In particular, highlighting tangible benefits may be more effective than discussing reduced risks. For example, benefits for private sector partners could include enhanced awareness of how their operations may be affected by disruptions to other systems and implications on business continuity planning; greater visibility into government planning efforts for mitigation, response, and recovery priorities; and deeper partnerships during steady-state with public sector counterparts. Benefits for government partners could include an improved understanding of the operational requirements of critical infrastructure and more realistic assumptions for disaster response and recovery; insights into possible cascading infrastructure failures; and deeper partnerships during steady-state with private sector counterparts.



### Ready for Next Step If You Have...

- Reviewed inputs for potential resilience assessment concept ideas
- Engaged informally with public and private partners on areas of potential shared interest that might be suitable for an assessment
- Identified a resilience problem for consideration in a potential resilience assessment

<sup>32</sup> CISA, *Fact Sheet on the National Risk Management Center*. November, 2018. Accessed February 13, 2020. [www.cisa.gov/publication/national-risk-management-center-fact-sheet](https://www.cisa.gov/publication/national-risk-management-center-fact-sheet).

## STEP 2 DESIGN ASSESSMENT



Once a regional infrastructure resilience problem has been identified and defined at a high level, the next step is to refine initial concepts into a viable assessment by defining specific research questions and identifying specific activities that will occur as part of assessment execution. The design phase sets the stage for everything that follows, including data collection, analysis, communicating results, and taking action to address infrastructure resilience gaps identified through the assessment.

### Refining an Assessment Concept

A general assessment concept (e.g., cyber threats to dams) requires refinement to define a clear research question that can drive assessment design and execution. Refining a concept for a resilience assessment into a specific research topic is an important precursor to more tactical scoping. This refinement process injects more specificity into a topic and makes it more relevant to the region. It begins to articulate clear knowledge gaps that an assessment is intended to address, which helps to identify the necessary analytic activities. In addition, the process of refinement allows regional partners to jointly discuss the outcomes that they want to achieve, which shape the assessment’s activities, analysis, and outputs. Figure 8 outlines a staircase process that begins with the identification of a general concept and culminates in research questions that in turn drive assessment scoping, data collection, analysis, and product development.



### Building an Assessment Team

The composition of the assessment team is strongly tied to the intended outcomes of the project and the type of analysis envisioned. Effective teams will pull in a portfolio of skills that is representative of the anticipated work in the assessment. They also typically will involve people from more than one agency or organization. Expertise needed to execute the assessment could come from a range of personnel, such as planners, engineers, hazard experts, data analysts, and project managers. Applicable skills include qualitative and quantitative analysis, oral and written communications, logistics, and technical expertise in a relevant topic area. When gaps in skills are identified, potential sources for additional expertise and bandwidth include local universities, federal personnel staffing regional offices, public-private partnership organizations, and other local or state agencies.



FIGURE 8.—Stepping Through Assessment Design.

### Moving from General Concepts to Specific Ideas

A broad, general topic is not suitable for guiding assessment design; it must be refined into a specific research topic. Focused topics for resilience assessments tie together subject areas, locations, and impact considerations, and they may consider both present concerns as well as future conditions. Table 3 provides some examples of both broad and focused topics that could inform regional infrastructure resilience assessments.

A focused topic should incorporate an implicit question or problem in need of solving. For example, in the last row in the table below, the focused topic implies that the impact of climate change on the substations is not known, which could be a concern to a variety of stakeholders and thus be a logical topic for a regional infrastructure assessment. A focused topic can be easily restated as a question. Adding “what is” to the beginning of the focused topic is a simple way to gauge whether a topic can become a viable assessment. If the question created is logical and answerable, the topic has potential; if it is not, further refinement of the topic is likely necessary.

**TABLE 3**  
**Examples of Assessment Concept Refinement**

Broad Topic	Focused Topic
<b>Drought and water supply</b>	The impact of drought on agriculture in the California Central Valley
<b>Failure of Dixon Canyon Dam</b>	The effect of the failure of Dixon Canyon Dam on lifeline infrastructure in Fort Collins, Colorado
<b>Water system cyber vulnerabilities</b>	The consequence of a cyber-disruption affecting automated processes for wastewater treatment in Cheyenne, Wyoming
<b>Electric grid and climate change</b>	The impact of climate change on high-voltage transmission substations in Massachusetts

## Selecting the Topic

The process of identifying one or more general concepts and refining them is likely to produce several focused topics that could be a suitable basis for an assessment. Selecting which to pursue is influenced predominantly by two factors: the perceived value in answering the underlying question, and the willingness and ability of stakeholders to provide a level of support necessary to do so.

The perceived value is a key factor in enlisting stakeholder support, so considering this element early in the assessment design process is advisable. A simple exercise to gauge the value of the potential assessment topic is to consider what would be lost if this question remains unanswered and who cares about the answer to this question. If the answers are “nothing” or “no one,” then this topic likely is not worth pursuing. The inverse possibility is partners arriving at focused topic(s) that are of mutual interest and value, but then finding the stakeholders needed to support the effort are unwilling or unable to do so. Many valid reasons exist for government and private sector reservations about participating in an assessment, including concerns about sharing sensitive data and information, apprehension about how widely findings (as well as the data used to inform these findings) will be shared, the existence of more pressing priorities, and resource constraints in terms of funding or personnel.

The ideal result of the concept identification and topic refinement process is that it yields an assessment topic that has agreement and support from relevant stakeholders. The most successful regional assessments are those that address a specific issue of mutual concern and shared interest among all stakeholders, as these topics foster the greatest enthusiasm and willingness to contribute.



### Understanding Time Horizons

Different types of assessments will require varying amounts of time to complete, depending on complexity, number of participants, and other factors. However, keeping in mind the voluntary nature of these efforts, the assessment process often must adapt to the timelines of outside organizations. An assessment can take weeks or months to complete, including development of final outputs. Desired outcomes can take longer, often years, to realize, particularly given the diversity of partners involved and the complexity of issues addressed.



### Incorporating Topics from Leadership

Organizational leadership may identify a regional infrastructure topic needing research and assessment, but the proposed topic may be broad or general in nature. The issue could emanate from a recent disaster, national level study, new law, or other sources. In such cases, the topic must be deconstructed, narrowed, and focused by analysts to better create the basis for a meaningful and executable assessment.

### Defining Specific Knowledge Gaps

An important factor for designing an assessment is defining specific knowledge gaps associated with a critical infrastructure resilience problem. These knowledge gaps can describe regional partners' blind spots in their understanding or planning assumptions and feed the development of research questions that an assessment is intended to address. Key stakeholders may have an incomplete awareness of their knowledge gaps. For example, partners may understand their dependencies on goods and services required for day-to-day operations, but they are unlikely to recognize the need to understand the vulnerabilities of the upstream infrastructure systems they depend on and the consequences of their disruption. These knowledge gaps

also can be useful factors to consider in the assessment design phase, where planning for more tactical issues on data collection and analysis are important. Some example knowledge gaps related to regional infrastructure resilience include the following:

- What are the most critical assets in this regional infrastructure system?
- What are key functions or services that support operations of this critical system?
- What are potential hazards that could cause a significant disruption to this infrastructure system? How likely are they?
- How will a disruption of one infrastructure asset/system affect another infrastructure asset/system?
- How dependent are operations of these infrastructure assets/systems on one another?
- How will a specific hazard (e.g., hurricane) impact these critical assets/systems?
- How will projected future environmental conditions affect infrastructure systems?
- How will incremental or fundamental evolution of related issues, including markets, regulation, and technological advancements, affect infrastructure systems?
- How vulnerable is the infrastructure system to a specific hazard?
- How will infrastructure dependencies across multiple sectors impact incident response and recovery activities?

### Articulating Desired Outcomes

Every assessment should begin with its outcomes in mind (i.e., the desired end-state that will result from its completion). Outcomes are the higher order aim of what the assessment endeavors to help its participants achieve; they speak to the underlying purpose of the effort. Where the topic, knowledge gap, and research questions define what the assessment will examine, the outcomes describe to what end these resulting insights will be applied. Desired outcomes are central to assessment design, informing everything from the partners involved to the nature of the end-products delivered. The following statements are representative of assessment outcomes:

- Inform emergency management organizations of the operational needs of critical water and wastewater systems in order to improve prioritization of assets following a disaster.
- Improve the cybersecurity of critical state government IT systems through the identification of vulnerabilities and their potential consequences and mitigation measures.
- Support community resilience planning initiatives through the identification of clusters of critical lifeline infrastructure to support neighborhood-level resilience planning initiatives.



### Anticipating Potential Barriers

Regional infrastructure assessments may not gain momentum for various reasons, such as:

- Another organization has primary authority and/or is already examining the topic.
- Essential partners are unable to adequately participate for various reasons.
- Topic has already been sufficiently studied.
- Insufficient time/resources.
- Topic does not align with leadership priorities.

Outcomes and outputs are not the same. Outputs are items produced during the course of the assessment (e.g., geospatial information, maps, reports) that are necessary or otherwise useful to achieving the outcome. Outcomes define the ultimate result of the actions taken during the course of an assessment. Outcomes inherently reach beyond the boundaries of the organization performing the infrastructure assessment and touch key partner needs.

## Developing Research Questions

With the assessment topic narrowed and desired outcomes identified, the next step entails identifying discrete research questions that stakeholders would like to answer in order to address knowledge gaps. Developing these questions is a critical part of assessment design and should be done early, as it protects against wasted time and effort in data collection and analysis and helps ensure that activities advance the collective understanding of the identified problem. Activities that do not assist in answering the research questions are extraneous to the assessment and should be avoided.



### Flexible Research Questions

While it is important to solidify these guiding questions as early as possible, in many cases the questions will be refined or even change somewhat as more is learned about the project topic. The complexity of infrastructure has a way of “hiding” issues that only come to light after more targeted examination. Remaining flexible with these research questions is therefore important.

At their core, research questions define what must be answered in order to address the assessment topic. Fundamentally, research questions establish the bridge between the starting point of a well-defined, narrow assessment topic and the desired outcomes. Developing research questions are valuable because they:

- Narrow the focus of the study but leave open the questioning;
- Subdivide research activities into manageable parts;
- Drive data collection; and
- Help organize outputs.

## Scoping Assessment Activities

With research questions in hand, the next step is to scope out what activities will occur through the assessment process to answer the research questions, including what data are needed, what analytic approaches are relevant and feasible, what potential outputs can lead toward desired outcomes, and who the target audience is.

A straightforward approach for scoping is to consider a collection strategy that outlines how to gather the necessary data and information and an analytical strategy to define what will be done with that data and information once collected. These factors will vary based on the desired outcomes of the assessment, the associated research questions, and the broad type of assessment being pursued. In the early stages of an assessment, those data collection and analysis strategies will likely be preliminary, but they should provide sufficient clarity to inform timelines, milestones, and outputs.



### Dangers of Skipping Research Questions

Failing to define a clear set of research questions is a risky path for regional infrastructure resilience assessments. Members of the project team may develop differing views of what the project is seeking to accomplish, which leads to confusing messaging, unclear guidance, and wasted effort. Project stakeholders may become frustrated with the lack of a clear vision for the assessment and may misunderstand their role in the process.

Issues to consider as part of the collection strategy include the following:

- What types of data are needed and why? How does it relate to the research questions? What approaches will the assessment team use to collect the data?



One resilience assessment project focused on an inland waterway navigation system originally planned to focus on resilience issues associated with aging infrastructure. However, while aging infrastructure remained a research question explored during the project, a different research question emerged that had not been considered a primary concern at the outset of the project: what is the risk of exposure to hazardous materials following barge accidents facing communities located near remote locks and dams? (CISA, *Resiliency Assessment: McClellan-Kerr Arkansas River Navigation System (MKARNS)*. March, 2019.)

- How long will it take to complete the data collection process? Are there certain times of year to target or avoid due to potential conflicts? (e.g., seasonal hazards, budget cycles, syncing with similar efforts)
- How easy will it be to use the data once collected? What is the format of available data, and what format do analysts need the data to have for use in the analysis? Is data available in a highly structured database with complete metadata for easy use, or will the data require manual extraction from reports and plans?

- Are any data quality requirements or considerations required? How up-to-date does the collected data need to be? Does the needed data change frequently?
- If planning data or data generated from modeling is collected from several sources, are the assumptions and data used in such modeling and planning consistent across the sources? What are the impacts of discrepancies?
- What is the availability of the needed data? Are the data available in public datasets? If not, would it be faster and less expensive to purchase proprietary data, if available, rather than collecting this information from several organizations? What limitations are associated with proprietary data? How would those limitations affect project outcomes?
- How will the data be used in the assessment? Will actual data need to be shared to achieve desired outcomes or is data only needed to inform analysis? Do any limitations exist on sharing or using collected data?
- Which partner/supporting organizations will need to be consulted or tapped to provide this data? Do relationships already exist with the necessary points of contact for those organizations and are they supportive of the effort? Will certain organizations need to be engaged before others?
- If interviews or questionnaires are planned, are existing question sets available that could be adapted for use? If using questionnaires, how will they be disseminated? How will the responses be compiled/stored to support analysis?
- What are the potential information security concerns associated with the data and information needed for the analysis?



In the case of the RRAP, one useful approach has been to identify broad categories of resilience assessments and apply them to project concepts to help frame major data collection, analysis, and product development efforts that are relevant. This simple analytical framework may be helpful for regions considering similar assessments, as it includes projects focused on characterizing infrastructure systems and projects centered on evaluating the consequences of infrastructure disruptions from different hazards. Together, these project types can help stakeholders begin to frame a roadmap for key activities that feed into regional infrastructure resilience assessment efforts.

- **Characterizing infrastructure systems:** The goal of characterization projects is to improve the baseline understanding of the infrastructure landscape. It can be considered a foundational analysis for regional and system resilience, which is essential to identifying potential system vulnerabilities and understanding and managing complex infrastructure risks. Understanding key inputs and outputs, system operations, important dependencies and interdependencies, critical system nodes, and risk exposures, as well as what encompasses structural and functional aspects of the infrastructure, fits in the scope of this type of resilience assessment answers “what are” questions about infrastructure systems (e.g., what are the critical transmission substations in a region?). By characterizing existing infrastructure systems, these projects provide a snapshot of “business as usual” operations of infrastructure.
- **Understanding consequences of disruption:** The goal of a consequence-focused project is to examine specific infrastructure-related risks and improve corresponding resilience planning and preparedness. A consequence-focused project identifies or evaluates the potential or actual effects of an event, incident, or occurrence. This type of project often includes an analysis of (a) the vulnerability of infrastructure systems in question, (b) a failure scenario or specific hazard with assumed or assessed effects on selected infrastructure in a region, and (c) prevention, protection, mitigation, response, and recovery capabilities of regional partners. This type of resilience assessment answers “what if” questions about infrastructure systems (e.g., what happens to the electric grid if an extreme, long-duration heat wave occurs?). By assessing the impacts of infrastructure disruptions, these projects provide an understanding of disrupted or alternative operations of infrastructure. These assessments may evaluate disrupted operations at a single point in time post-disruption or evaluate the impact of infrastructure disruptions in a dynamic manner.

Characterization-focused assessments can include straightforward depictions of individual infrastructure systems as well as more complex efforts that reflect the high degree of interconnectedness that is typical of modern infrastructure systems. Consequence-focused projects typically involve more in-depth analysis than characterization projects because they layer in hazard analyses with the core understanding of infrastructure system operations.

Issues to consider as part of an analysis strategy focus on anticipating how the team can obtain the desired analysis outputs using the data collected. The analytic techniques selected will vary based on the identified research questions, the availability of required data, the tools and methodologies available to the organization, the capabilities of analysts in the organization, and the time and resources available.

- What analytic techniques, tools, and methodologies will be needed to obtain the desired analysis outputs? Are they accessible to the necessary analysts?
- Will any modeling be necessary? What data are required and is it reflected in the collection strategy?
- How long will it take to complete the analysis?
- How will the data be shared and visualized to support analysis/interpretation? What assistance/capability is required to perform this visualization?
- Will any external third-parties be required to complete this analysis? If so, are they aware of the requirement and willing to assist? What mechanisms are required to enable this analysis and are they already in place (e.g., non-disclosure agreement)?
- Will the analysis require validation by another party? If so, who?
- Who is the audience for this analysis? What is the right level of technical detail to convey to them?
- Does the analysis have phasing considerations? Will results of the first phase of analysis inform the types, extent, and scope of additional analysis required?

As these activities are defined, they can form the basis of a project plan that analysts can use to manage the overall effort. In addition to the overarching goals, objectives, and research questions of the assessment, a project plan should highlight what activities are occurring when; what the important milestones are; what the key outputs will be; how the assessment team will collaborate throughout the life of the effort (e.g., monthly meetings, weekly calls); and how draft and final materials will be shared and with whom. These collection and analysis considerations can also inform the identification of a core assessment team that will help establish a collaborative approach among regional partners to executing the assessment, facilitate continuous engagement with stakeholders, manage a realistic schedule and budget, and ensure leadership awareness of major accomplishments and challenges.



## Developing a Project Plan

DHS recommends that every RRAP project team develop a project plan that documents the overarching goals of the project and the key steps needed to accomplishment. Topics typically addressed in these project plan include the following:

- Project description
- Key scoping elements (e.g., sectors, geographic area, threat/hazard)
- Purpose and objectives
- Audience
- Research topic
- Research questions
- Analysis methodology
- Outputs
- Implementation activities
- Timeline
- Key points of contact
- Partner organizations
- Knowledge management

An important factor to consider in scoping and throughout the process is remaining cognizant of the amount of time that is required to conduct effective assessments. For example, DHS’s RRAP projects can take 18-24 months to complete the scoping, data collection, analysis, and product development phases. That extended time horizon may not be practical or desired in all cases, given resource constraints and time pressures that organizations face from internal and external sources. Keeping the overall objectives of the assessment process at the forefront can help the assessment team hedge against scope creep and stay on track in terms of budget and schedule.

### Research Planning Techniques

The process for planning a regional assessment of critical infrastructure follows the general process for planning any research project. At its core, research planning involves understanding what questions need to be answered and devising a feasible technical approach for doing so, taking into account internal and external schedule, capability, and resource constraints. Given these similarities, techniques used in the research planning process (e.g., concept mapping) may be useful to the team engaged in planning a regional assessment. Notably, the techniques most suitable for this type of assessment work will be qualitative and mixed-method approaches that involve both quantitative and qualitative analysis.



### Hosting a Formal Kickoff Meeting

Key stakeholder buy-in is critical to project success. It is oftentimes helpful to hold a formal kick-off meeting attended either in-person or virtually by federal, state, local and private sector stakeholders who have been pre-identified as being integral to the assessment. The kick-off meeting can be a platform to build consensus and momentum for the assessment and to show that each stakeholder has a critical role in the success of the project. In addition to presenting the initial scope and goals, additional participants could be identified, opportunities for the project team to participate in upcoming exercises and events could be discussed, and agreement could be reached on project timeline, initial data collection, and possible outputs.



### Ready for Next Step If You Have...

- Defined specific knowledge gaps
- Defined research questions
- Identified desired outputs and outcomes
- Established an assessment team to manage the process
- Socialized assessment concept with key stakeholders and outlined anticipated activities
- Developed a project plan and strategies for data collection and analysis
- Hosted a kickoff meeting

# STEP 3 COLLECT DATA



The data used to support resilience assessments can be extremely diverse, including qualitative and quantitative information collected through various methods. The data itself could include structured quantitative data sets, geographical information, plans and procedures (e.g., business continuity and emergency operations plans), lists of facilities or suppliers, narrative reports, or notes from meetings and interviews. Analysts must collect and review disparate data sets for multiple infrastructure sectors in order to build a body of resources that can feed resilience analysis activities.

Data collection includes activities ranging from open-source research and literature reviews that occur remotely without stakeholder input to in-person interviews, workshops, and site visits that require direct discussions with stakeholders. Analyzing the resilience of infrastructure systems in a region often requires analysts to identify and use an array of data collection activities throughout the duration of the assessment. Together, these data collection activities allow analysts to develop a more refined, accurate, and comprehensive basis for understanding a region’s infrastructure, its operations, backup capabilities, critical dependencies and interdependencies, disaster-related concerns, and other related issues.

Of utmost importance is the need to be respectful of the time and effort being requested of participating entities. Key to this is keeping data collection focused only on the information required for analysis (versus “nice to have” information that is not directly relevant; here again, having well-composed research questions will assist greatly) and clearly managing expectations about time commitments, topics for discussion, intended use of and procedures to protect data collected, and expected outcomes through clear and continuous communication.

Team members should have a clear sense of what information is truly needed for the assessment and what information is secondary, minimizing the burden on participants and building trust with partners. Similarly, it is important to align the skills and abilities of team members with different data collection

approaches. For example, different skillsets are required for conducting one-on-one interviews with technical personnel, facilitating workshops with groups of senior managers, leading assessments, and identifying open-source data inputs.



## Respecting Partners’ Time

Strategies for engaging partners effectively and respectfully in data collection include the following:

- Be prepared with questions that can be reasonably answered within the time available.
- Share topics for discussion with partners in advance.
- Ensure that partners understand the goals of the engagement and how their information fits in.
- Be organized, efficient, and respectful of participants’ time.
- Communicate expectations clearly in advance, especially about types of personnel being sought for inclusion (e.g., operations, security).
- Allow time for partners to ask questions and discuss the overall objectives.

The following sections describe example approaches for collecting relevant data. Depending on the nature of the topic being assessed and the scope of the inquiry, certain data collection methods may be more applicable or effective than others for a given assessment. However, in all cases, data collection approaches must align with the desired outcomes of the assessment and be designed to support them, as documented in a project plan. Prior to embarking on a data collection process, organizations pursuing regional infrastructure resilience assessments must begin with an exploration of information security rules, requirements, and mechanisms in order to ensure that potentially sensitive data are protected in accordance with partner needs and applicable laws and guidelines.



### Addressing Stakeholder Concerns

Potential assessment partners may express significant concerns about information protection. Strategies for openly discussing and addressing those concerns include explaining the following:

- What the intended use of the data is
- Why that information is important
- How the data will be protected
- Whether anonymizing inputs (e.g., non-attribution, generalized observations) is an option
- What the final products will be and how they will reflect the data
- How the final products will be protected and why/how that level of protection may differ from that of the original data
- What data protections are available and what information qualifies for it

## Information Security

Before embarking on any data collection activity, assessment teams must consider the information security implications for each activity and the data to be collected. An effective data collection strategy is enabled by forethought on information security, as it allows assessors to anticipate some reservations that potential partners may have about sharing information and think through the mechanisms available to protect the collected information that would mitigate their concerns. These concerns also apply to data generated through analysis processes.

Key partners in regional infrastructure resilience assessments may be interested in developing and sharing completely open-source assessment outputs (e.g., reports, brochures, briefings) that can be disseminated without limitation. In other cases, the information used to inform the assessment or the results that it generates may be sensitive in nature. For example, data inputs collected through resilience assessments may be proprietary, business sensitive, For Official Use Only (FOUO), Protected Critical Infrastructure Information (PCII), or other designations used by different nations or organizations. In some cases, this information may be protected from disclosure either under the Freedom of Information Act or state sunshine laws. Purchased proprietary data or data protected by non-disclosure agreements may carry significant legal and financial penalties if intentionally or accidentally disclosed.

A transparent decision process for determining information security requirements should be documented and applied before data collection even begins. These considerations include understanding the intrinsic sensitivity of the information being collected, whether it is available in the public domain, and how combining it with other data sources might affect protection requirements. These considerations apply to all outputs generated during the course of an assessment, including final reports, facilitated discussion or workshop slide presentations, technical papers, brochures and handouts, fact sheets, interview notes, geospatial and visualization products, and workshop after-action reports. Decision points to consider include the following:

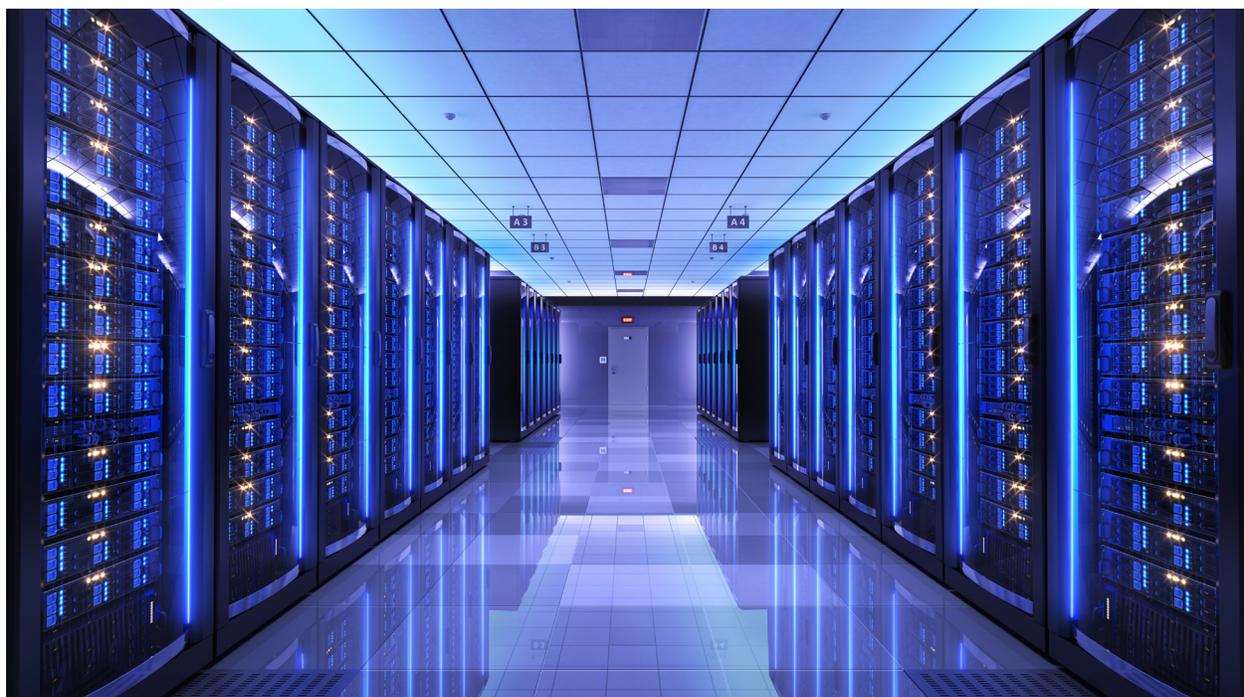
- Is the information in the public domain?
- Was the information obtained from sources originally marked or designated as sensitive or restricted? (e.g., PCI; Sensitive Security Information related to transportation security; FOUO; Critical Energy/Electric Infrastructure Information (CEII) for critical energy-related information; internal proprietary information shared with consent by participating organizations)
- Was the information provided with an expectation of protection?
- Does the product reveal any sensitive information that might be impacted by relevant laws or federal directives?
- What are the relevant state laws and associated rules on ensuring public access to government records?
- Who will manage the collected data, and what procedures will they use to protect the data?
- Do parties involved understand how to protect sensitive information and what the ramifications could be if it is not protected properly?
- What are the intended outcomes of the assessment? (e.g., public planning process or more close-hold applications) How do those outcomes affect the type of information that can be incorporated into assessment outputs?

Finally, given the voluntary nature of these types of assessments, instances may exist where partners will ultimately decide not to share select types of data under any conditions, regardless of any security or legal protections that are offered.



### Balancing Goals of Information Protection and Information Sharing

Assessments will often face the competing needs of protecting certain information versus sharing results as broadly as possible. In most cases, assessments are intended to convey knowledge as widely as possible to inform inter-organizational planning and educate numerous stakeholders. Therefore, assessment planning must grapple with how best to do this while simultaneously ensuring required information protection.

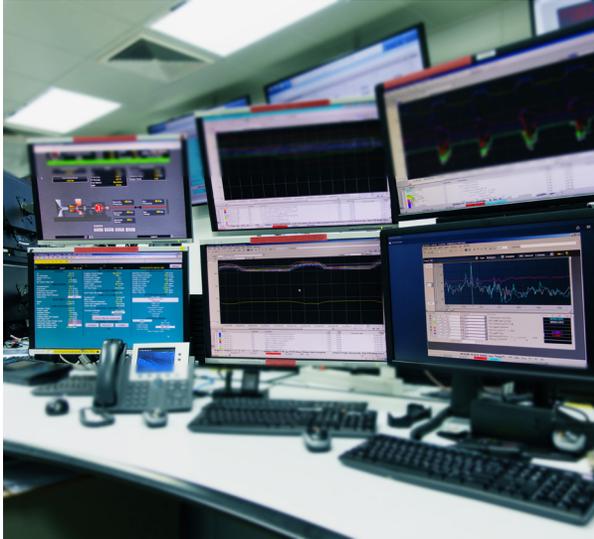




## Information Security Regimes

A number of programs and policies exist to control the dissemination of sensitive but unclassified information related to critical infrastructure.

- **For Official Use Only (FOUO):** a designation for documents with unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest. Documentation from DHS on FOUO is available here: [www.dhs.gov/publication/security-1](http://www.dhs.gov/publication/security-1).
- **Protected Critical Infrastructure Information (PCII):** a designation for private sector infrastructure information voluntarily shared with the government for the purposes of homeland security. Critical infrastructure information is information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records or other information. Information from DHS on PCII is available here: **Change URL to** [www.cisa.gov/pcii-program](http://www.cisa.gov/pcii-program).
- **Chemical-terrorism Vulnerability Information (CVI):** the information protection regime administered under the Chemical Facility Anti-Terrorism Standards (“CFATS”) regulation to ensure information chemical facilities provide to DHS is protected from public disclosure or misuse. Information on CVI is available here: [www.cisa.gov/chemical-terrorism-vulnerability-information](http://www.cisa.gov/chemical-terrorism-vulnerability-information).
- **Sensitive Security Information (SSI):** information that, if publicly released, would be detrimental to transportation security, as defined in 49 CFR part 1520. Information from DHS on SSI is available here: [www.tsa.gov/for-industry/sensitive-security-information](http://www.tsa.gov/for-industry/sensitive-security-information).
- **Critical Energy/Electric Infrastructure Information (CEII):** information related to proposed or existing critical electric infrastructure that includes specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual). Information from the Federal Energy Regulatory Commission on CEII is available here: [www.ferc.gov/legal/ceii-foia/ceii.asp](http://www.ferc.gov/legal/ceii-foia/ceii.asp).
- **Law Enforcement Sensitive (LES) Information:** unclassified information used by law enforcement personnel that requires protection against unauthorized disclosure to protect the sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.
- **Traffic Light Protocol (TLP):** TLP is a set of designations used by CISA to ensure that sensitive information is shared with the appropriate audience. TLP provides a simple and intuitive schema, but is not a “control marking” or classification scheme. Information about TLP is available here: [www.cisa.gov/tlp](http://www.cisa.gov/tlp).



## Data Collection Methods

The sections that follow explore a spectrum of different approaches to collecting data, including: literature reviews; open-source research; controlled datasets; multi-organizational facilitated discussions; one-on-one interviews; structured surveys and assessments; exercises; and plan reviews.



## Interacting With Voluntary Partners

Voluntary assessments can provide numerous benefits, but a fundamental challenge is that key participants can choose to step away at any point. This is especially relevant to infrastructure owners/operators that are likely short on time. Interactions with these participants need to be well organized and concise. The purpose needs to be clear and agreed upon, and these participants should fully understand the end goals and why their participation is important.

## Literature Review

A literature review is a common first step in a qualitative and quantitative research process where analysts identify a body of relevant publications—including books, journal articles, and analytic reports—and review them to identify previously documented observations, and conclusions, and remaining unanswered questions. In research projects, the literature review process often concludes in a summary document that characterizes existing research and associated findings. Conducting a literature review early in the assessment process has several important benefits. First is that a search of relevant information sources will help determine what is already known about the topic and how extensively the topic has already been researched, helping analysts refine the analytical plan.

Next, a literature review can quickly reveal which researchers have written the most on a particular topic, potentially identifying experts for consultation on the assessment's topic. Similarly, a literature review can identify important data sources used previously by other researchers. Using the same data sources can introduce efficiencies and enhance consistency. For example, applying the same seismic scenario used in an ongoing state planning process in a regional infrastructure resilience assessment introduces an immediate opportunity to augment concurrent state planning activities with assessment results.

Finally, identifying methodologies used in past studies of the same or similar topics is often a useful outcome. In addition to identifying previous work, a literature review could help elucidate an alternative approach for the assessment based on observations about the advantages or challenges associated with methods used in previous research. Finally, identifying relevant peer-reviewed publications will also add a degree of technical rigor.<sup>33</sup>

Table 4 outlines potential benefits and drawbacks to using literature reviews as a data collection approach in a regional infrastructure resilience assessment.

<sup>33</sup> Van Wee, Bert, and David Banister, "How to Write a Literature Review Paper?" *Transport Reviews*, 36:2, 278-288. 2016. DOI: 10.1080/01441647.2015.1065456.

**TABLE 4**

**Examples of Assessment Concept Refinement**

Benefits of Literature Reviews	Drawbacks to Literature Reviews
<ul style="list-style-type: none"> <li>■ Can be conducted remotely, without demands on stakeholder time</li> <li>■ Identifies vetted research, data sources, assessment models and methodologies, analytical findings, and subject matter experts on relevant topics</li> </ul>	<ul style="list-style-type: none"> <li>■ May not identify issues or results that are tailored to a specific region (i.e., analytical results may not be good predictor of expected analytical results of similar analysis in a different region)</li> <li>■ More academic than operational or practical in nature</li> <li>■ Not grounded in stakeholder needs and operational experience (e.g., aggregate information rather than stakeholder-specific)</li> </ul>

**Open-source Research**

The goals of open-source research are similar to those of a literature review. However, while a review of the literature is generally considered to be a compilation of the research that recognized scholars and researchers have published on a topic, open-source research broadens that search beyond published journal articles and books to include other types of information in the public domain.

The term open-source generally refers to publicly available information appearing in print or electronic form. This includes the Internet (e.g., online publications, blogs, social media), media (e.g., newspaper and magazine articles), public government data (e.g., reports, speeches, websites, regulatory compliance filings), commercial data (e.g., business market research reports, databases), gray literature (e.g., technical reports, patents, white papers, unpublished works, newsletters, industry press releases, corporate presentations), and professional and academic publications (e.g., journal articles, conference proceedings, dissertations).

Open-source information may have unlimited dissemination to a broad public audience (e.g., mass media) or more controlled dissemination to a more select audience (e.g., company shareholder reports). Whatever form it takes, open-source materials generally do not intentionally include information that is restricted or is subject to proprietary constraints beyond copyright.<sup>34</sup> However, experienced open-source researchers may realistically find instances where an

organization has inadvertently posted sensitive or proprietary materials online for public view. In these cases, stakeholder engagement meetings focused on reviewing and validating publicly available data provide an opportunity to draw partner attention to these disclosures and discuss reasons for potentially protecting such information rather than sharing it openly.

Additional challenges with using open-source data are data integrity and data validity. Analysts should exercise caution when using old sources or sources without a publication date. Where possible, analysts should validate data with relevant stakeholders, especially when dealing with unvalidated data or data published by an unverified source. Data that are consistent across multiple open sources may increase the likelihood of data validity. Analysts should remain vigilant since several sources may simply show data based on a single source.

Furthermore, analysts should carefully consider the potential motivations and biases of publishers of open-source data. Identifying potential biases, whether intentional or not, is critical to limiting explicit and implicit bias in all phases of resilience assessments. For example, bias in research that a special interest group conducts can influence research assumptions, scope, analysis scenarios, methodologies, and presentation of results.

Table 5 outlines potential benefits and drawbacks to using open-source research as a data collection approach in a regional infrastructure resilience assessment.

<sup>34</sup> Steele, Robert David, "Open Source Intelligence," in Loch Johnson (ed.), *Handbook of Intelligence Studies* (NY: Routledge, 2007).

**TABLE 5**

## Considerations for Open-Source Research in Data Collection

Benefits of Open-Source Research	Drawbacks to Open-Source Research
<ul style="list-style-type: none"> <li>■ Can be conducted remotely, without demands on stakeholder time</li> <li>■ Extends beyond academic literature into other publicly available data sources</li> <li>■ Involves a range of techniques of varying sophistication (e.g., simple Internet searches, web scraping, access to open data libraries)</li> <li>■ Prepares analysts for more targeted data collection and stakeholder engagement activities</li> </ul>	<ul style="list-style-type: none"> <li>■ Requires additional reviews to ensure validity of information and reliance on trusted sources</li> <li>■ May uncover sensitive information that requires follow-up with pertinent organizations</li> </ul>

### Accessing Controlled Datasets

Numerous public and private entities have created structured, curated datasets that may not be available publicly but are potentially valuable sources of information to factor into regional resiliency assessments. For instance, some federal entities have comprehensive datasets that may be available to select partners for regional assessments if they can establish a clear need. Examples include energy data submitted to the Federal Energy Regulatory Commission, waybill data with the U.S. Department of Transportation (DOT), waterborne commerce data from the U.S. Army Corps of Engineers (USACE),

and select geospatial layers included in the secure component of Homeland Infrastructure Foundation-level Data (HIFLD). In addition, private companies collect and organize datasets related to various infrastructure functions and make these resources available for purchase. Commercial data and business analytics toolsets, visual products to analyze electric power systems, and telecommunications databases are examples of resources available through private partners.

Table 6 outlines potential benefits and drawbacks to accessing controlled data sets in a regional infrastructure resilience assessment.

**TABLE 6**

## Considerations for Accessing Controlled Datasets in Data Collection

Benefits of Controlled Datasets	Drawbacks of Controlled Datasets
<ul style="list-style-type: none"> <li>■ Can be accessed and reviewed remotely, without demands on stakeholder time</li> <li>■ Can be compared to and combined with open-source information</li> <li>■ Enables access to validated and structured datasets from trusted sources</li> </ul>	<ul style="list-style-type: none"> <li>■ May have legal stipulations or costs associated with access</li> <li>■ May involve sensitive information</li> <li>■ May restrict options for sharing analytic products derived from the data</li> </ul>

## Multi-organizational Facilitated Discussions

A facilitated discussion will typically involve numerous participants from the spectrum of regional stakeholders engaged in an assessment, including different levels of government, private sector, and researchers. These discussions can have various purposes, including identification and validation of infrastructure data including critical dependencies and independencies across organizations and sectors, as well as cross-sector stakeholder engagement and information sharing that can effectively “fill the gaps” in knowledge between individual organizations. This process helps to identify cascading impacts that might not surface otherwise, as well as potential solutions that require review from multiple perspectives.



### Scheduling Facilitated Discussions

Facilitated discussions can be used effectively at different stages in an assessment. They can be used early on to gather a cross-section of views about the topic and enable a more refined approach to data collection. They can be used midway through an assessment to gauge progress and begin identifying final points of focus for assessment outcomes. They can also be used at the end of an assessment to explore outcomes and consider next steps. The common characteristic is that they pull together multiple organizations at once to advance the overall effort.

While facilitated discussions are often structured as scenario-based conversations that a facilitator leads, they do not necessarily align with practices outlined in the Homeland Security Exercise and Evaluation program (HSEEP), nor are they intended to operate as Federal Advisory Committee Act committees. During these meetings, a facilitator

guides the discussion using one or more scenarios with additional subject matter experts as needed. Participants are briefed on supporting infrastructure and operating environment from a preliminary analysis of existing information; issues and proposed resilience solutions are also reviewed with participants. The results of a facilitated discussion can help identify “strings to pull” during future data collection and analysis.

Examples of the types of general questions posed at a facilitated discussion are listed below. The discussion should be constructed in a way that addresses key research questions of the assessment; specific objectives for the type of information intended to be elicited should inform the planning and preparation for the event. Facilitated discussions present an opportunity to further explore unexpected responses from participants to prepared questions and uncover unknown factors that should inform the resilience assessment.

- How exposed or vulnerable are relevant infrastructure systems to the threat/hazard used in the scenario?
- How would the scenario described affect the critical infrastructure systems in question? What are the consequences of those effects?
- How might other dependent or interdependent critical infrastructure be affected directly by the threat/hazard or indirectly by the disruption of another critical infrastructure system?
- How would participants respond to these events?
- What opportunities do they see as having potential to mitigate the effects of a disruption to one or more infrastructure systems?
- What are the biggest obstacles to improving the resilience of stakeholders’ infrastructure systems? What outcomes of the regional resilience assessment would be of most value to stakeholders and help them close resilience gaps?
- What are participants’ existing plans, strategies, or capabilities to deal with the consequences? Are these mechanisms sufficient? If not, what challenges arise from insufficient planning and capability development?<sup>35</sup>

<sup>35</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).



## Re-engaging Stakeholders Through Workshops

The length of time between project initiation and completion can exceed 1 year. As the data collection phase progresses, it can be challenging to keep all participants engaged. However, individual data collection activities may highlight issues relevant to many or even all participants. This can provide an opportunity to reengage stakeholders collectively through a workshop to provide new insights on the assessment topic, and generate additional group discussion that can inform future data collection activities and final assessment outcomes.

Table 7 outlines potential benefits and drawbacks to using facilitated discussions as a data collection approach in a regional infrastructure resilience assessment.

**TABLE 7**  
**Considerations for Facilitated Discussions in Data Collection**

Benefits of Facilitated Discussions	Drawbacks to Facilitated Discussions
<ul style="list-style-type: none"> <li>■ Collaborative opportunity for stakeholders who may not typically work together</li> <li>■ Efficient way to engage with multiple stakeholders in one setting</li> <li>■ Grounded in technical specifics of the systems/region at hand</li> <li>■ Informal dialogue allows for flexible lines of questions and enables the moderator to encourage conversation</li> </ul>	<ul style="list-style-type: none"> <li>■ May be limited to specific scenario(s) used to frame discussion</li> <li>■ Tightly scoped to accomplish specific priorities in a short period of time</li> <li>■ Can require significant up-front planning time and logistical considerations</li> <li>■ Participants may be unwilling to share important data due to presence of customers or competitors for fear of business implications</li> </ul>

### One-on-One Interviews

In some cases, more in-depth interviews with one or more subject matter experts may be needed. The participants will depend on the goals and objectives of the data collection process and may include local utilities, local or regional government entities, and/or system and infrastructure owners that are the focus of the assessment. Guided by

question sets prepared in advance, interviews may be conducted to validate preliminary analysis results, determine areas of concern or critical nodes/assets, understand how business operations function in steady-state, and collect relevant plans and documents as needed (e.g., business continuity plans, system models and operating procedures, regional emergency plans, and continuity of government plans).

One-on-one interviews present an opportunity for participants to plan in advance to ensure that personnel from all areas of expertise (e.g., operations, management, planning) are present to lend expertise to answering relevant questions. Interviews provide opportunities to discuss topics in a smaller venue that may have arisen during facilitated discussions and merit follow-up, or that may not be appropriate for discussion in a group environment (e.g., proprietary or otherwise sensitive business practices, specific vulnerabilities or resilience issues). One-on-one interviews can be conducted in person or remotely, but participants may be more willing to share sensitive data in person

rather than over the phone. When conducted in person, this approach can also incorporate tours of infrastructure facilities that can convey uniquely valuable insights about facility operations, dependencies, vulnerabilities, hazard exposure, disaster concerns, emergency plans, and related topics. Tours will often unveil new issues and considerations for incorporation into the assessment strategy and plan.

Table 8 outlines potential benefits and drawbacks to using one-on-one interviews as a data collection approach in a regional infrastructure resilience assessment.

**TABLE 8**  
**Considerations for Interviews in Data Collection**

Benefits of Facilitated Discussions	Drawbacks to Facilitated Discussions
<ul style="list-style-type: none"> <li>■ Potential to be conducted remotely</li> <li>■ Opportunity for focused engagement with technical experts</li> <li>■ Discussion questions tailored to specific data needs</li> <li>■ Generates more granular data on topics of interest</li> <li>■ May facilitate more candid information sharing</li> </ul>	<ul style="list-style-type: none"> <li>■ Can be time-consuming for assessment team and stakeholders</li> <li>■ Requires significant up-front planning to develop questions and schedule meetings</li> <li>■ May introduce information security issues depending on data collected and stakeholder preferences</li> </ul>



### Identifying Appropriate Interviewees

One-on-one interviews, either in-person or by phone, can be one of the most effective methods of collecting valuable insights. However, infrastructure owners/operators, industry groups, and government agencies are often large organizations with many components. Efforts must be made to identify the specific sub-groups and individuals that are capable of addressing specialized issues within an assessment. It is not unusual to have an introductory meeting, and then a more focused follow-up with additional experts once the interviewee better understands the scope.

## Structured Surveys and Assessments

Depending on identified requirements, other data collection activities may include the use of structured assessment tools or custom surveys that employ a repeatable methodology to collect a common set of data points about facilities, systems, jurisdictions, or issues. These structured assessments could be self-assessments that an entity conducts on its own or facilitated assessments implemented in conjunction with government partners or private subject matter experts. The purpose is the same as facilitated discussions and one-on-one interviews: collect information on critical assets/nodes and their role in a system’s resilience, and to fill data/information gaps for analysis as it relates to the assessment scope. A number of specialized field assessments can be used either independently or in conjunction with individual owners and operators to identify vulnerabilities, dependencies, interdependencies, capabilities, and cascading effects of impacts on the critical infrastructure in different sectors. A regional resilience assessment could involve reviewing results from recently completed surveys and assessments or identifying additional locations for focus where surveys and assessments have not yet occurred.

Assessments can be employed effectively to support regional resilience assessments in several ways:

- **Deriving trends from a large set of previously conducted assessments of similar facilities in order to produce generalized observations on common, average, or exceptional security features, resilience characteristics, vulnerabilities:** This approach is most effective when seeking characterization type information about a type(s) of infrastructure present in a region, and where they are perhaps too numerous to assess individually as part of the assessment. When working across large geographic regions with large numbers of assets, this is a valuable approach. For example, this approach could be used to identify the typical electric power dependency profile of communications assets in order to better understand how they would be effected by a large power outage.

- **Performing a series of assessments on a representative or otherwise prioritized sampling of similar infrastructure in a region in order to identify common issues, trends, or notable variance in their security or resilience:** This approach is most useful when attempting to characterize infrastructure security and resilience using regionally specific assets and information. This information can then be generalized to represent other similar assets in the region. It also allows for individual asset to asset comparison that can identify more specific gaps or trends in need of addressing. For example, conducting the same assessments at each of the five largest water treatment plants in a region could help regional risk managers and emergency planners identify common security issues needing attention or important operational requirements of each facility post-disaster.
- **Performing a limited number of assessments on certain assets that system-level analysis has identified as being particularly critical to the overall function of the system within which they operate or to one or more systems with which they interact:** If particularly important assets are identified, the natural question is to what extent are they protected or prepared and what more can be done to improve their security and resilience. This approach works in concert with system and system of systems level analysis, and can help articulate the consequence of asset specific vulnerabilities and capability gaps, as their exploitation can lead to disruptive events impacting other interconnected assets/systems. For instance, if an analysis of bulk fuel movements into a metropolitan area identified two terminals that were responsible for the overwhelming majority of fuel distribution, assessments could be performed on them to identify how secure and resilient to disruption they are and what issues concerning their continued operation exist.

Table 9 highlights some example assessment processes led by federal organizations that can feed into broader regional resilience assessments. These types of assessments may require advance coordination to schedule and maybe offered in finite quantities based on personnel availability through established processes.

**TABLE 9**

**Example Voluntary Infrastructure Assessment Processes**

Sponsoring Organization	Assessment	Description
CISA	Infrastructure Survey Tool (“IST”)	A voluntary, web-based security survey called the Infrastructure Survey Tool that CISA’s Protective Security Advisors conduct in coordination with facility owners and operators across the country to identify and document the overall security and resilience of the facility <sup>36</sup>
CISA	Cybersecurity Assessments	A range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. Example assessments include Vulnerability Scanning, Phishing Campaign Assessment, Risk and Vulnerability Assessment, Cyber Resilience Review, External Dependencies Management Assessment, Cyber Infrastructure Survey, Remote Penetration Testing, Web Application Scanning, and Cyber Security Evaluation Tool (CSET®)
Environmental Protection Agency	Climate Resilience Evaluation and Awareness Tool (“CREAT”)	A risk assessment application that helps utilities to adapt to extreme weather events by better understanding current and long-term weather conditions.
U.S. Department of Health and Human Services	Healthcare and Public Health Risk Identification and Site Criticality (“RISC”) Toolkit	Data-driven all-hazards risk assessment with three self-assessment modules focused on identifying threats and hazards, assessing vulnerabilities, and evaluating criticality and consequences
U.S. Coast Guard (USCG)	Maritime Security Risk Analysis Model (“MSRAM”)	Assessment to understand and mitigate risk of terrorist attacks on targets in U.S. ports and waterways

<sup>36</sup> CISA’s Protective Security Advisors are trained subject matter experts in critical infrastructure protection and vulnerability mitigation who facilitate local field activities in coordination with other DHS offices. They also advise and assist state, local, and private sector officials and critical infrastructure facility owners and operators. Information is available at: [www.cisa.gov/protective-security-advisors](http://www.cisa.gov/protective-security-advisors).

Table 10 outlines potential benefits and drawbacks to using facility assessments as a data collection approach in a regional infrastructure resilience assessment.

**TABLE 10**  
**Considerations for Facility Assessments in Data Collection**

Benefits of Facility Assessments	Drawbacks to Facility Assessments
<ul style="list-style-type: none"> <li>■ Opportunity for focused engagement with key personnel at facility of interest</li> <li>■ Yield detailed, structured, and comparable information about security and resilience issues at a facility that may be representative of regional trends</li> <li>■ May incentivize future participation in broader regional activities</li> </ul>	<ul style="list-style-type: none"> <li>■ Can be time-consuming for assessment team and stakeholders</li> <li>■ Facility-level assessments may be of limited use to broader regional evaluations; limited to established methodology</li> <li>■ May introduce information security issues depending on assessment focus</li> <li>■ May be limited in availability and require coordination with sponsoring agency</li> </ul>

### Exercises

Exercises can be an immensely valuable opportunity for data collection. These can be arranged specifically for the assessment, or they may already be scheduled and can simply incorporate the assessment team as observers. In the case of the latter, exercises oriented around a similar scenario, infrastructure system, or other subject relevant to the scope

of the assessment provide an ideal opportunity to observe discussions or operations of the participants, which may produce helpful insights for the assessment. The research, plans and other exercise material assembled in preparation for the exercise can also be used to support the assessment. Lastly, the after-action reports generated from these exercises may document observations about infrastructure and organization performance that can inform the assessment.



### About HSEEP

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Exercises are a key component of national preparedness: they provide participants from across the whole community with the opportunity to shape planning, assess and validate capabilities, and address areas for improvement. HSEEP can assist exercise program managers in developing, executing, and evaluating exercises that address the priorities established by an organization’s leaders. Additional information about HSEEP is available at [www.preptoolkit.fema.gov/web/hseep-resources](http://www.preptoolkit.fema.gov/web/hseep-resources).

Planned exercises and real-world incidents also provide opportunities for learning and adaptation. For example, fuel shortages after Hurricane Sandy illustrated the interdependencies and complexities of infrastructure systems, the challenges in achieving shared situational awareness during large events, and the need for improved information collection and sharing among government and private sector partners to support restoration activities. The critical infrastructure and national preparedness communities conduct exercises on an ongoing basis through the National Exercise Program and other mechanisms to assess and validate the capabilities of organizations, agencies, and jurisdictions.

During and after planned and no-notice events, partners identify individual and group areas for improvement, implement and evaluate corrective actions, and share best practices with the wider critical infrastructure and emergency management communities.<sup>37</sup> These findings can be valuable inputs to the data collection process. FEMA’s HSEEP can be a useful tool in designing and implementing exercise programs. CISA’s exercise program also provides support to government and private sector stakeholders.

Table 11 outlines potential benefits and drawbacks to using exercises as a data collection approach in a regional infrastructure resilience assessment.

**TABLE 11**  
**Considerations for Exercises in Data Collection**

Benefits of Exercises	Drawbacks to Exercises
<ul style="list-style-type: none"> <li>■ No-fault opportunity to test existing plans/procedures and explore logical dependency considerations</li> <li>■ Identify strengths and areas for improvement that can inform key findings in broader assessment process</li> </ul>	<ul style="list-style-type: none"> <li>■ Requires significant up-front planning and logistics</li> <li>■ Focus of existing exercises may not align completely with overall assessment objectives</li> <li>■ Inherent artificiality of exercises may not sufficiently test operational concerns associated with infrastructure systems</li> </ul>



One assessment project focused on the resilience of the petroleum supply chain in New Jersey. The team conducted a tabletop exercise to explore critical information sharing needs and mechanisms between private sector partners and the state emergency operations center during a significant weather event. The exercise also allowed private sector partners to review standard operating procedures for pre-storm, during storm, and post-storm status reporting in support of response and recovery efforts, as well as to examine the cascading effects of cross-sector critical infrastructure disruptions within New Jersey. (CISA, *Resiliency Assessment: New Jersey Petroleum*. April, 2015.)

<sup>37</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

## Plan Reviews

The analysis of existing plans and procedures can help assessment teams identify priorities and gaps. For the purpose of regional infrastructure assessments, two broad categories of plans are valuable for review purposes: emergency plans and steady-state plans. Plans that describe what actions to take when an event occurs (e.g., emergency operations or contingency plans) are important when trying to understand the potential consequences of disruptions and how various partners will respond. For example, states usually have a comprehensive emergency management plan that could be consulted. These are plans that would be activated to coordinate resources to support activities related to such critical assets, such as those providing fuel and power supplies, during an event. These plans help the state provide coordination of

the response and recovery efforts and assist in supporting local jurisdictions based on their agencies’ or organization’s unique areas of expertise, resources, and authorities. Among other ways, they can also serve as a valuable data collection resource in terms of identification of planning gaps, dependent partners, operational timeframes, and other factors. Alternately, steady-state plans focus on longer-term activities during non-disaster situations (e.g., hazard mitigation, long-term transportation planning). These resources are helpful for understanding the configuration, operations, and challenges of the existing infrastructure systems.

Table 12 outlines potential benefits and drawbacks to using plan reviews as a data collection approach in a regional infrastructure resilience assessment.

**TABLE 12**  
**Considerations for Plan Reviews in Data Collection**

Benefits of Plan Reviews	Drawbacks to Plan Reviews
<ul style="list-style-type: none"> <li>■ Can be conducted remotely, without demands on stakeholder time</li> <li>■ Grounded in existing documentation and real-world processes</li> </ul>	<ul style="list-style-type: none"> <li>■ May not be current or reflect lessons from recent incidents</li> <li>■ Possible that no relevant plan exists to address regional concerns</li> <li>■ May contain unidentified gaps due to lack of testing or real world implementation or not being maintained (i.e., out of date)</li> </ul>



### Ready for Next Step If You Have...

- Confirmed the types of data that are needed to support relevant analysis approaches
- Identified which stakeholders to engage for which types of data
- Conducted open-source research to minimize impact on stakeholders
- Developed interview questions and facilitated discussion materials as needed
- Determined what data can be shared with whom and under what circumstances
- Implemented information security practices as appropriate
- Completed relevant data collection activities needed to support analysis

# STEP 4 ANALYZE



As data collection activities conclude, assessment activities can increasingly focus on applying different analysis techniques to begin to uncover answers to identified research questions. Some lines of analysis will likely have been planned during the assessment design phase. However, additional opportunities for analysis often emerge during the data collection process, complementing and amplifying analytic approaches planned earlier. In other cases, assessment teams may determine that previously proposed analysis may ultimately not be possible based on the actual data collected through stakeholder outreach and related research.

The analytical complexity of regional infrastructure resilience assessments will vary significantly based on a variety of factors including the footprint of the region itself, available resources (including expertise and funding), time constraints, data availability, desired applications for the results, and overall management objectives. Regional partners must adjust the overall analytic approach based on changes to these factors over the course

of the assessment in order to achieve actionable results that balance analytical needs with real-world resource constraints. Table 13 illustrates how analysis activities can be scaled to range from simpler approaches to more advanced ones based on the types of issues being explored (e.g., characterizing infrastructure systems, understanding consequences of disruptions).

**TABLE 13**  
**Scaling Analysis Approaches for Regional Infrastructure Resilience Assessments**

Characterizing Infrastructure Systems	
Foundational Analysis	Geospatial data layers of infrastructure systems
Intermediate Analysis	Geospatial mapping of infrastructure systems and hazards
Advanced Analysis	Dashboard or infographic product that facilitates dynamic analysis of infrastructure systems subject to hazards or other impacts
Understanding Consequences of Disruption	
Foundational Analysis	Interviews with owner operators or experts
Intermediate Analysis	Modeling of impact to single infrastructure system
Advanced Analysis	Modeling of impact to system of systems, including cascading failures

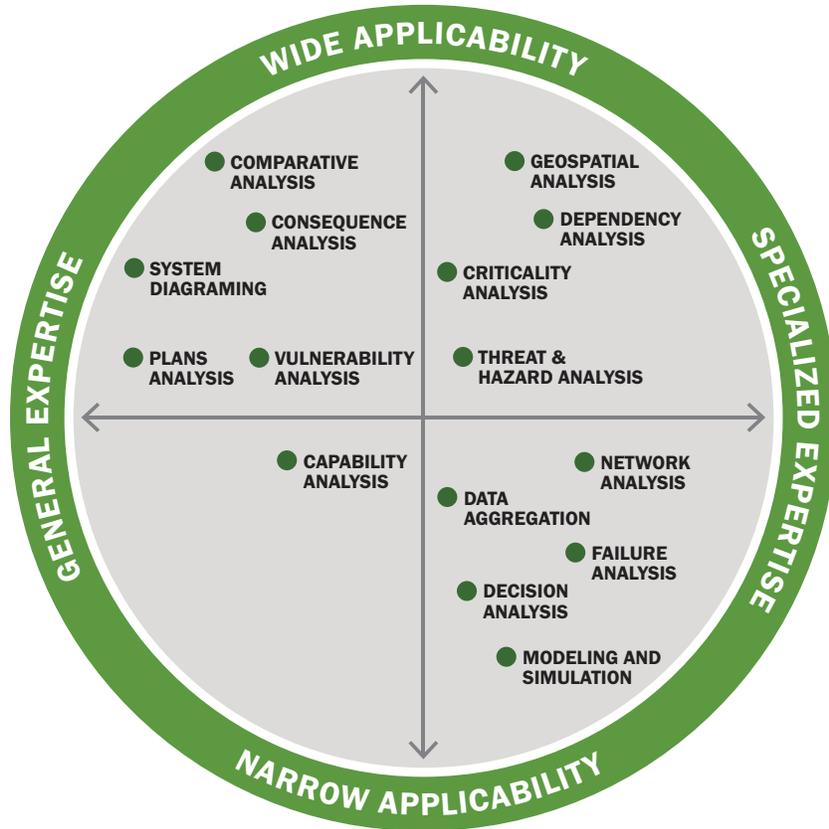


FIGURE 9.—Understanding Relevance of Different Resilience Analysis Techniques.

In general, regional resilience analyses will incorporate numerous analytic techniques. Capabilities in these areas will likely hail not just from the primary organization spearheading the assessment, but from multiple organizations with relevant expertise, including federal, state, and local governments; university and research organizations; and other partners. Some of these analytic approaches have widespread applicability across many different potential assessments while others are more narrowly tailored to specific use-cases. Similarly, some approaches can be accomplished by analysts with a more

general skillset grounded in critical thinking and practical understanding of infrastructure systems operations; others may require more advanced technical skills in data science, engineering, geographical information systems, or other specialized areas. Figure 9 illustrates where different analysis techniques fall on these spectrums.

Figure 10 shows how teams can apply multiple analytic techniques to address a particular research question and generate outputs for stakeholders.

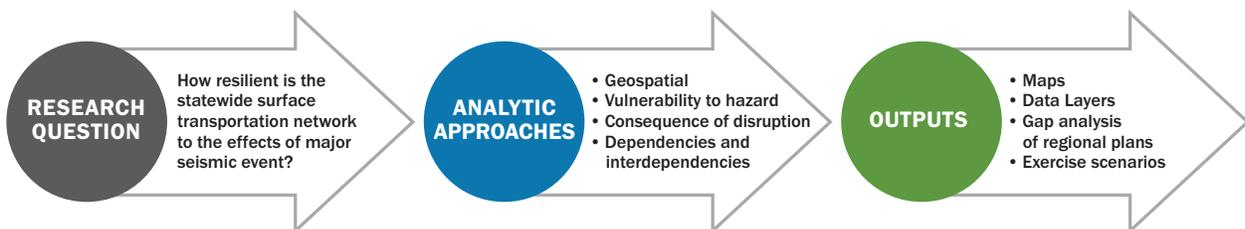


FIGURE 10.—Linking Research Questions, Analytic Approaches, and Outputs.

The sections that follow explain the importance of adhering to analytic standards and then provide general descriptions for each of the techniques outlined in table 14 and recent examples of how they have been applied in example resilience assessments through the RRAP.

**TABLE 14**  
**Analytic Approaches for Regional Infrastructure Resiliency Assessment**

Type of Analysis	Description
<b>Dependency Analysis</b>	Evaluate how individual assets, systems, and networks interact to understand how complex systems operate and discern the potential consequences of a disruption
<b>Consequence Analysis</b>	Identify or evaluate the potential or actual effects of an event, incident, or occurrence
<b>Threat and Hazard Analysis</b>	Identify or evaluate entities, actions, or occurrences that have or indicate the potential to harm life, information, operations, and/or property
<b>Vulnerability Analysis</b>	Identify physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards
<b>Criticality Analysis</b>	Identify, evaluate, and prioritize based on the importance of an impact to mission(s), function(s), or continuity of operations
<b>Comparative Analysis</b>	Conduct detailed, side-by-side review of two or more variables, data sets, processes, or systems in order to identify similarities and differences
<b>Geospatial Analysis</b>	Use geospatial information (i.e., data associated with particular locations) and associated visualization tools to model or create mathematical representations of real-world systems
<b>System Diagramming</b>	Develop visualizations of the components of a system and the connections (logical or physical) among them that define how the system operates
<b>Capability Analysis</b>	Identify specific capabilities required to address a given threat or hazard in terms of planning, organization, training, equipment, and exercise elements and evaluate readiness to deliver those capabilities in a timely manner when requested
<b>Plans Analysis</b>	Review strategic, operational, or tactical plans from multiple jurisdictions in order to identify gaps and overlap
<b>Data Aggregation</b>	Use statistical processes to combining disaggregated data in order to assess specific trends for one or more parameters
<b>Network Analysis</b>	Evaluate a system of interconnected elements that represent possible paths across an ecosystem of nodes and links
<b>Failure Analysis</b>	Collect and analyze data to determine why an entity, asset, system, or network experiences a failure in operations
<b>Modeling and Simulation</b>	Use a conceptual representation of a system (e.g., physical, mathematical, logical) to imitate how it would function in a real-world context in order to improve decision making
<b>Decision Analysis</b>	Apply a systematic and logical set of procedures for analyzing complex, multiple-objective (multi-criteria) decision problems

## Adhering to Analytic Standards

Before embarking on the analysis phase of an assessment of regional infrastructure resilience, it is important to consider existing standards of analytic tradecraft and incorporate them into the overall approach for the analysis. Research and analysis organizations in government and academia follow intellectual and analytic standards in order to preserve the integrity of their work and ensure that the results are defensible.

Of particular note are the analytic standards that the U.S. intelligence community follows. Initially established in 2007 and revalidated in 2015, these analytic standards govern the production and evaluation of analytic products, and they articulate the responsibility of intelligence analysts to strive for excellence, integrity and rigor in their analytic thinking and work practices.<sup>38</sup> Although regional infrastructure assessments are not typically intelligence-focused, these standards provide a valuable framework that translates well into the assessment process, as they define important steps to creating credible and defensible results. The policy directive for the intelligence community on analytic standards also serves as a common foundation for developing education and training in analytic skills across the research and analysis community, including for public and private partners engaged in resilience assessment. The directive highlights the nine analytic tradecraft standards:

- Properly describe the quality and credibility of underlying sources, data, and methodologies;
- Properly express and explain uncertainties associated with major analytic judgments;
- Properly distinguish between underlying intelligence information and analysts' assumptions and judgements;
- Incorporate analysis of alternatives;
- Demonstrate customer relevance and address implications;
- Use clear and logical argumentation;
- Explain change to or consistency of analytic judgements;

- Make accurate judgments and assessments; and
- Incorporate effective visual information where appropriate

Additional information on these analytic standards is publicly available from the Office of the Director of National Intelligence for review and integration into assessment planning by regional partners in government, private sector, and non-profit and academic institutions.

## Dependency Analysis

Dependency analysis is at the core of regional resilience assessments because, as a risk multiplier, dependencies and interdependencies are central to understanding and analyzing resilience. Dependency analysis fundamentally explains how many individual assets, systems, and networks present within the region of study interact, and these interactions are what enable analysts to convey how these complex systems operate and discern the potential consequences of a disruption. A threat or hazard can result in the loss of a service (e.g., electric outage), potentially affecting the critical infrastructure requiring this resource for operation, which further impacts other critical infrastructure dependent upon that infrastructure's services. The total consequences of an event are amplified by the dependencies and interdependencies that exist among critical infrastructure facilities and systems.

The difference among the assessment types and their treatment of dependencies is the scale and degree to which this examination occurs. A characterization assessment might identify important dependencies within a critical system; discuss their importance to the system's function; and generally address potential risks arising from those dependencies that could result in a system disruption. A consequence-focused assessment uses dependencies to identify and analyze the cascading effects of a failure scenario or hazard's impact on one or more critical infrastructure systems. The level of dependency analysis performed varies depending on the assessment's scope, ranging from general (i.e., identify rough estimates of probable cascading effects across

<sup>38</sup> DNI (Office of the Director of National Intelligence), *Intelligence Community Directive 203: Analytic Standards*. January 2, 2015. Accessed February 13, 2020. [www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf](http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf).

many sectors) to highly focused (i.e., understand how a specific hazard affecting one system will impact operations of another highly dependent system). Table 15 outlines four distinct classes of infrastructure dependencies and

interdependencies that are helpful in scoping, executing, documenting, and communicating analysis: physical, cyber, geographic, and logical dependencies.<sup>39</sup>



The fact that disruption of certain critical components of a system can lead to overall system-level and cascading failures was clearly demonstrated by the New York City electricity network (and other utilities) during Hurricane Sandy. During and after the storm, one-third of the city's electric generating capacity was temporarily lost. Five major electric transmission substations in the city flooded and shut down. Parts of the natural gas distribution network were inundated. Four out of six steam plants in the city were knocked out of service. By the time the storm passed, more than 800,000 customers (representing more than 2 million New Yorkers) were without power, and 80,000 customers were without natural gas service. A third of the buildings served by the city's steam system—including several major hospitals—were without heat and hot water. Generally, damaged substations were repaired quickly, with power restored to most customers in Manhattan, for example, within 4-5 days. Repairing damage to the whole overhead system, though, took almost 2 weeks, even with the help of thousands of utility workers from other states. Damage to electrical equipment within buildings took considerably longer in many cases. (City of New York, *PlanNYC: A Greener, Greater New York*. 2013. Accessed February 13, 2020. [www1.nyc.gov/site/sirr/report/report.page](https://www1.nyc.gov/site/sirr/report/report.page).)

<sup>39</sup> Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, Vol. 21, No. 6 (2001), 11–25. Accessed February 13, 2020. <https://ieeexplore.ieee.org/document/969131>.

**TABLE 15**  
**Dependency and Interdependency Classes**

Class	Description	Example
<b>Physical</b>	Operations depend on material output(s) of or services provided by other infrastructure through a functional and structural linkage between the inputs and outputs of two assets. A commodity produced by or service provided by one infrastructure is needed as an input by another infrastructure for its operation.	Electricity is transmitted to a commercial building for functions such as lighting, heating, and running computers.
<b>Cyber</b>	Operations depend on information and data transmitted through the information infrastructure via electronic or informational links. Outputs from the information infrastructure serve as inputs to other infrastructure; the relevant commodity is information.	A SCADA system that monitors and controls infrastructure processes such as water treatment.
<b>Geographic</b>	Operations depend on the local environment, where an event can trigger changes in the state of operations in multiple infrastructure assets or systems. A geographic dependency occurs when infrastructure assets are in close spatial proximity (e.g., a joint utility right-of-way).	A joint utility trench containing gas, electric, and water lines in close proximity.
<b>Logical</b>	Operations depend on the state of other infrastructure via connections other than physical, cyber, or geographical. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes.	Security and geopolitical factors that influence the planning and operational decisions of energy infrastructure owners and operators.



A project involving an infrastructure interdependency analysis in Puerto Rico following Hurricane Maria assessed the potential propagation and consequences of cascading failures across dependent and interdependent lifeline infrastructure in order to inform recovery investments. Providing information on which infrastructure asset disruptions lead to the widest downstream impacts can be a useful way to prioritize capital investments and other mitigation efforts. Analysts determined the service areas of lifeline infrastructure (i.e., electrical, communications, water, and wastewater) using a spatial interaction model called the Huff Model. Commercial entities often use this technique to predict how many customers will visit particular retail stores; its application in this instance identified service areas for infrastructure assets. When the asset (e.g., an electrical substation) serving an area was disrupted, all of the customers in that area, including other infrastructure (e.g., a water treatment plant that depends on electricity from the disrupted substation) were also disrupted. The result is a cascading failure in other infrastructure service areas which, in turn, impacts more downstream users. (CISA, *Puerto Rico Infrastructure Interdependency Assessment: Community Lifelines Case Study Report*. August, 2019.)

In addition to classification of dependencies and interdependencies, attributes of these relationships must be gathered to answer the analytic questions and understand dependent and interdependent relationships. This information can be collected through

a variety of approaches, including facilitated discussions, one-on-one interviews, facility assessments, or (in some cases) open-source research. Table 16 outlines the most basic, but useful, attributes to consider in dependency analysis.

**TABLE 16**  
**Key Questions to Inform Dependency Analysis**

Key Questions	Attributes to Consider
<b>What</b> is the material or service that is needed?	<ul style="list-style-type: none"> <li>Characterize the dependency at a level of specificity beyond the sector and with quantitative features on volume and consumption rates (i.e., not energy, but fuel, or ultra-low sulfur diesel petroleum fuel or 600 gallons of ultra-low sulfur diesel per day.)</li> </ul>
<b>Why</b> is the material or service required?	<ul style="list-style-type: none"> <li>Describe the critical functions or processes supported by the resource in order to better understand the potential consequences associated with its loss and gauge how important the resource is to sustaining key functions</li> </ul>
<b>Who</b> provides this material or service to the facility?	<ul style="list-style-type: none"> <li>Understand alternate suppliers with whom infrastructure owners have established formal and information relationships to provide backup services</li> <li>Consider “who” and “where” separately; with distributed global supply chains, the physical location of the entity providing the resource may be different than the location from which the material or service originates</li> </ul>
<b>Where</b> does this material or service come from?	<ul style="list-style-type: none"> <li>Use location information to depict regional supply chains and identify geographic and physical dependencies related to the delivery route; knowing where a resource comes from is closely associated with understanding how it is provided (i.e., via rail, road, air, maritime transportation) and whether critical failure points exist along the route</li> </ul>
<b>How</b> is this material or service provided?	<ul style="list-style-type: none"> <li>Use this knowledge to identify additional first-order dependencies that support the delivery of these critical material and services. (e.g., if chemicals are a critical material for a facility and are delivered by rail, then the facility has a dependency on both its chemical supplier and the freight rail operator that delivers them)</li> </ul>
<b>When</b> is this material or service provided?	<ul style="list-style-type: none"> <li>Identify temporal factors that influence how critical a dependency is and the consequences of its loss; evaluate extent to which just-in-time delivery operations could impact resilience</li> <li>Understand differences between cases where continuous delivery of a resource is required for the system to maintain operations (e.g., Internet, fuel) and those where a resource delivery is needed only periodically (e.g., monthly resupply)</li> <li>Disruptions to resources delivered continuously may have a more immediate or significant impact than those on an extended resupply schedule; however, disruptions occurring near scheduled resupply windows when inventories are low may have greater effects, particularly in extended response and recovery operations</li> </ul>

The required data inputs, relevant qualitative and quantitative analytical techniques, and resulting products from dependency and interdependency analyses differ across the four classes of physical, cyber, geographical, and logical dependencies. Other dimensions that influence the scope and complexity of analysis include the following:

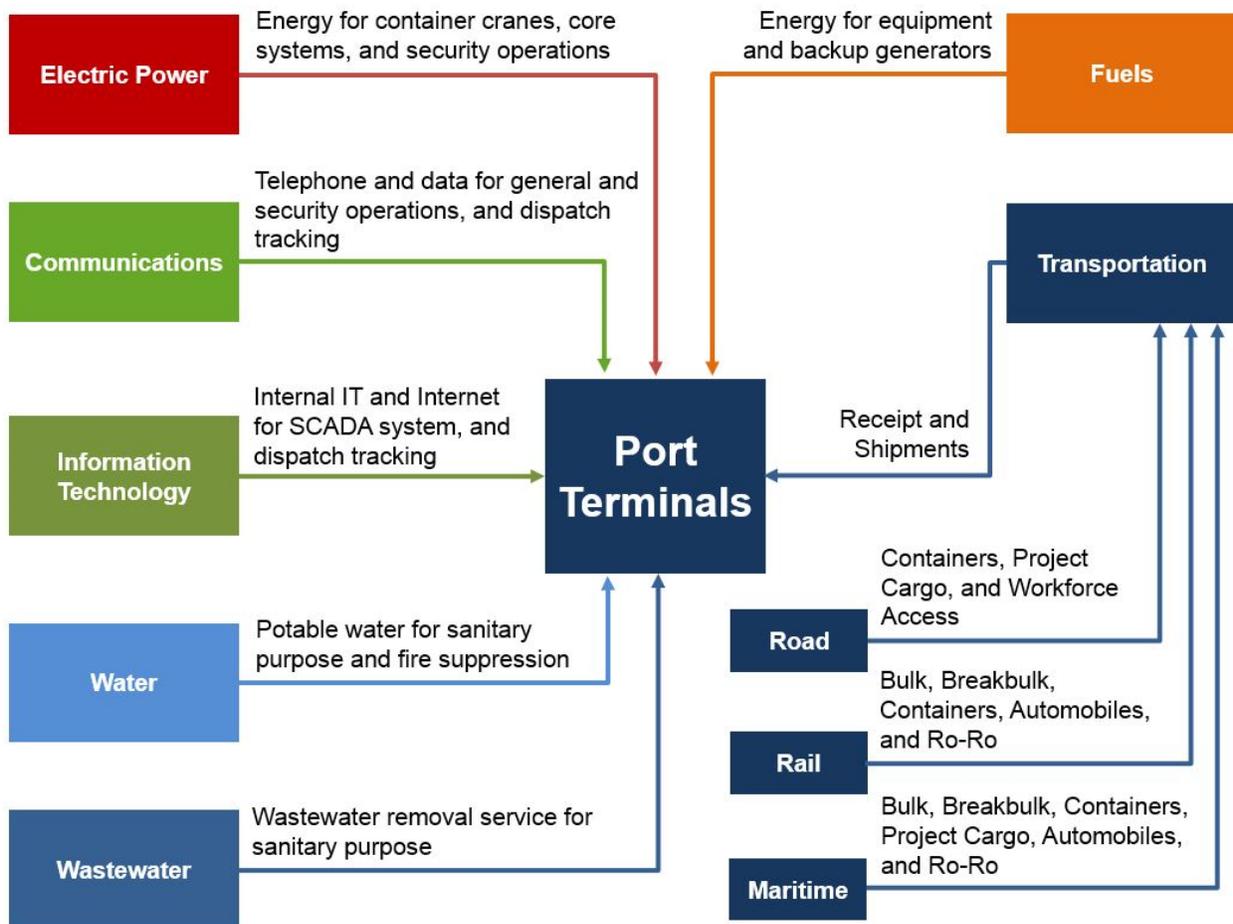
- Operating environment for critical infrastructure, including broader business, policy, legal, security, safety, and political considerations;
- Dynamic coupling and response behavior(s) for critical infrastructure following a disruption;
- Type(s) of failure affecting critical infrastructure;
- Infrastructure characteristics that influence the effects of a disruption; and
- State of operations for critical infrastructure (e.g., normal day-to-day operations, degraded operations).

Infrastructure dependency and interdependency analysis can be complicated, which, in turn, can limit the application of this information by stakeholders to make risk-informed decisions that enhance resilience. A “system of systems” approach can help establish the appropriate scope of a dependency analysis, as well as the specific assets and/or subsystems for which resilience-related information should be collected. Using this approach, analysis would consider the high-level context (e.g., a geographic region or an industry sector) and the associated states of these systems, ultimately represented by the most critical assets that will inform the scope and focus of a resilience assessment, including the most critical assets from which to collect dependency data.





A project involving an infrastructure interdependency analysis in Puerto Rico following Hurricane Maria assessed the potential propagation and consequences of cascading failures across dependent and interdependent lifeline infrastructure in order to inform recovery investments. Providing information on which infrastructure asset disruptions lead to the widest downstream impacts can be a useful way to prioritize capital investments and other mitigation efforts. Analysts determined the service areas of lifeline infrastructure (i.e., electrical, communications, water, and wastewater) using a spatial interaction model called the Huff Model. Commercial entities often use this technique to predict how many customers will visit particular retail stores; its application in this instance identified service areas for infrastructure assets. When the asset (e.g., an electrical substation) serving an area was disrupted, all of the customers in that area, including other infrastructure (e.g., a water treatment plant that depends on electricity from the disrupted substation) were also disrupted. The result is a cascading failure in other infrastructure service areas which, in turn, impacts more downstream users. (CISA, *Puerto Rico Infrastructure Interdependency Assessment: Community Lifelines Case Study Report*. August, 2019.)



## Consequence Analysis

Consequence analysis is the process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.<sup>40</sup> Human consequences can include fatalities and injuries resulting from an event. Economic consequences can include direct and indirect effects on a region’s economy. Mission consequences center on the ability of an entity to meet a strategic objective (e.g., national defense) or perform an important function (e.g., generating electric power, ensuring access to clean drinking water). Psychological consequences speak to the negative impacts of an event on the mental or emotional state of individuals or groups in an area, which can result in a change in perception and/or behavior. Consequence analysis is an important feature of regional resilience assessments, considering the effects arising from potential infrastructure disruptions. Depending on the data available and the tools used, consequences can be characterized qualitatively through relative rating approaches (e.g., high, medium, low) or in more precise quantitative measures (e.g., financial costs, lives lost).

Consequences can be direct or indirect in nature. A direct consequence is an effect that is an immediate result of an event, incident, or occurrence. Direct consequences can include injuries, loss of life, onsite business interruption, immediate remediation costs, and damage to property and infrastructure as well as to the environment. An indirect consequence is an effect that is not a direct consequence of an event, incident, or occurrence, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions. Examples of indirect consequences can include the enactment of new laws, policies, and risk mitigation strategies or investments, contagion health effects, supply-chain economic consequences, reductions in property values, stock market effects, and long-term cleanup efforts. Indirect consequences are important because they may have greater and longer-lasting effects than the direct consequences.<sup>41</sup> Indirect consequences

may manifest themselves through first-, second-, and third-order dependencies either upstream or downstream among infrastructure assets and systems.



An RRAP project analyzed how inundation resulting from high discharge at Table Rock Dam in Missouri could affect critical assets, systems, and nearby communities, helping them understand the consequences associated with downstream flooding. The CISA team focused on understanding how the White River System (particularly near the City of Branson) might behave following high-discharge events from Table Rock Dam, looking at a range of possible flood events and leveraging information from the City of Branson, the National Inventory of Dams, USACE, U.S. Geological Survey, Missouri Water Science Center, and publicly available information on past flooding events. The consequence analysis included a temporal component, allowing stakeholders to see how the flooding severity changed during the course of a scenario that covered 21 days. (CISA, *Resiliency Assessment: Branson, Missouri*. October, 2017.)

When analyzing the potential or actual consequences of infrastructure disruptions, it is important to account for both the localized impacts of a disruption occurring at a single asset (e.g., what are the effects on the individual asset? On the system of which it is a part? On the community in which it is located?), as well as the broader implications of that disruption at a regional scale and across one or more infrastructure systems (e.g., what are the effects on downstream consumers of the material or service associated with the asset? On other infrastructure systems? On other communities that rely on related infrastructure services or material?). The interconnectedness and geographical distribution of infrastructure systems means that a disruption at one asset

<sup>40</sup> CISA, *DHS Risk Lexicon: 2010 Edition*. September, 2010. Accessed February 13, 2020. [www.cisa.gov/dhs-risk-lexicon](http://www.cisa.gov/dhs-risk-lexicon).

<sup>41</sup> Ibid.

may have the potential to cascade across multiple systems through a domino effect. For this reason, consequence analysis and dependency analysis are tightly linked. Understanding the dependencies within and across systems allows assessment teams to better understand, predict, and minimize the consequences of disruptions.



The Cajon Pass is a vital corridor between Southern California and the rest of the Nation. Energy, communications, and transportation infrastructure (i.e., road and rail lines carrying goods to and from the Ports of Los Angeles and Long Beach) cross it. Given this importance, an RRAP project assessed impacts of major earthquake at the southern San Andreas Fault on these essential systems. As part of the project, the CISA team used a variety of data sources (including inputs from the USACE, U.S. DOT Surface Transportation Board and Federal Highway Administration) and off-the-shelf modeling via IMPLAN to estimate the economic impacts of a curtailment of rail and truck freight movements. The analysis showed that damage to the transportation infrastructure traversing Cajon Pass would reduce road and rail capacity, and would raise the cost of transporting goods as a result of switching to higher-cost alternative transportation routes. Indirect impacts would result from spending reductions on materials, equipment, and services in support of production as well as port operations, and from reduced wages and salaries. These impacts would also reduce tax revenue to local, county, and state governments. (CISA, *Resiliency Assessment: Cajon Pass*. November, 2015.)

## Threat and Hazard Analysis

A hazard is defined as a natural or human-caused source or cause of harm or difficulty. In particular, a natural hazard is a source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena. A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area by an adversary, while a hazard is not directed.<sup>42</sup> Many regional resilience assessments have a generalized hazard or scenario in mind that forms the basis of the analysis (e.g., the study of the dependence of a critical industry on electric power is undertaken because the industry is concerned about losing power due to a hazard). However, consequence-focused analyses generally focus on a specific threat (e.g., a cyber attack on the industrial control systems of a critical infrastructure asset or system) or hazard (e.g., Category 3 hurricane impacting a port).

Regional assessments of infrastructure resilience—as executed through programs like the RRAP—typically do not focus on determining whether a threat exists or a hazard is relevant outside of the problem identification and scoping phases of the assessment. The point of departure is that other analyses have established the relevance of a given threat or hazard; the goal is not to evaluate the likelihood of a threat or hazard occurring, but rather to focus on infrastructure’s exposure to those phenomena and the potential consequences of disruptions they may cause. These inputs can inform—but do not take the place of—comprehensive risk assessments that explore threat, vulnerability, and consequence factors along with the likelihood or probabilities associated with these factors.

<sup>42</sup> CISA, *DHS Risk Lexicon: 2010 Edition*. September, 2010. Accessed February 13, 2020. [www.cisa.gov/dhs-risk-lexicon](http://www.cisa.gov/dhs-risk-lexicon).



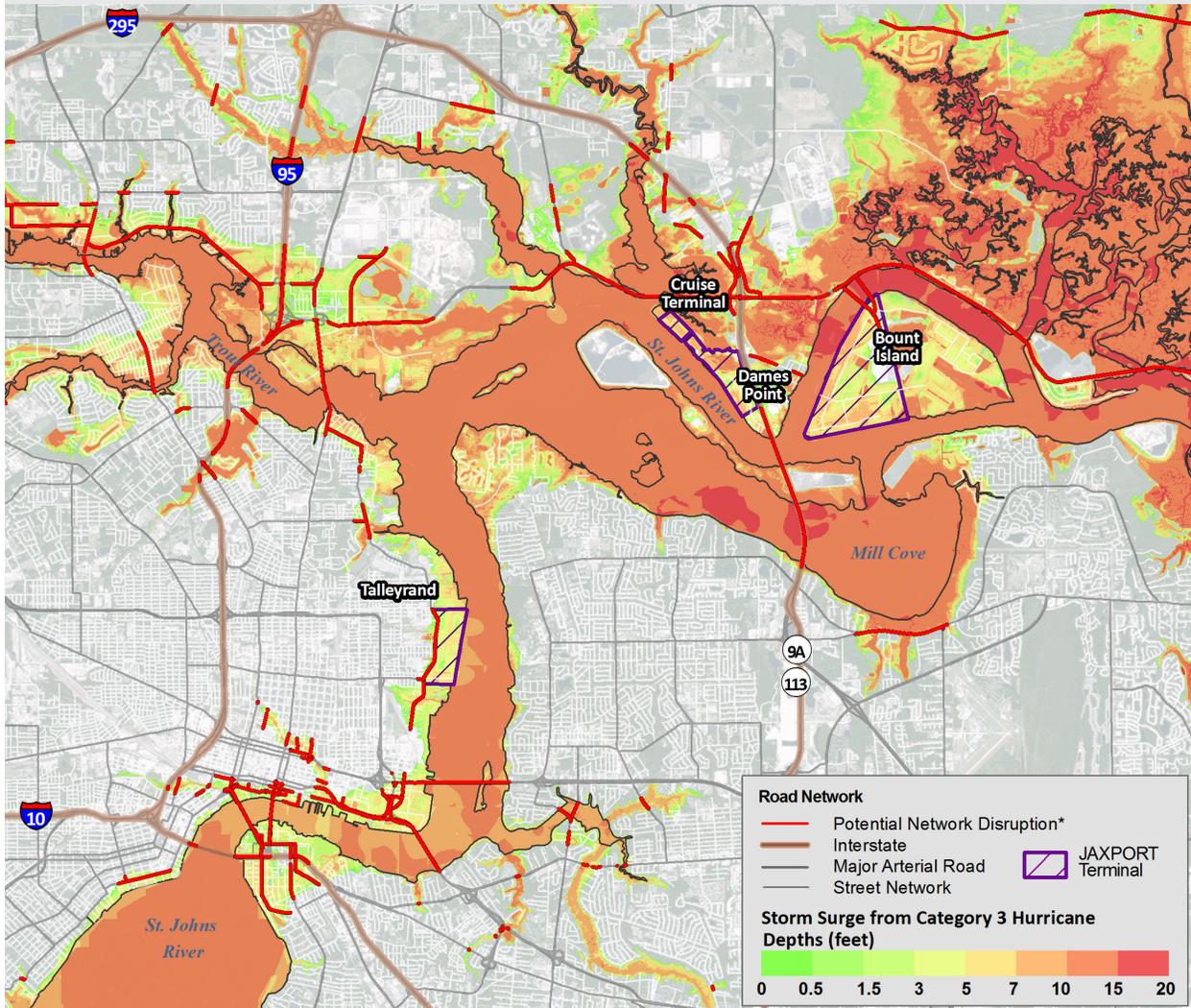
To incorporate threats and hazards into a regional resilience analysis, it is important to understand the nature of the threat or hazard, how it will manifest, and what effect it is expected to have upon the infrastructure at issue. In this way, threat and hazard analyses are inextricably linked with vulnerability analysis. Different levels of threat and hazard analysis can be applied, depending on the scope of the assessment and the degree of complexity desired. The first level is a top-line assessment of the infrastructure's exposure to the threat or hazard. This screen is helpful when seeking to establish a foundational understanding of possible risks to infrastructure systems that impact resilience. The aim is not to understand precise impacts, but simply to understand whether the potential for impact exists. Examples of this approach to threat and hazard analysis include the following:

- Determining the degree to which an infrastructure system relies on Internet-enabled industrial control systems, which suggests general exposure to and possible disruption from cyber threats; and
- Determining the geographic extent of expected floodwaters and identifying what infrastructure assets are located therein, which indicates potential for general flood damage and operational disruptions.

The second level focuses on a more detailed analysis of the threat or hazard in question and the vulnerability of the infrastructure to it. This level may also include analysis of the potential consequences associated with those vulnerabilities, both to the infrastructure itself and other dependent infrastructure. This approach requires a deeper technical understanding of the threat or hazard, and of the infrastructure itself. Keeping with the examples above, this more in-depth approach would require understanding specific cyber threats and the technical vulnerabilities of the actual systems in use; in the second case, the approach would involve modeling flood behavior based on environmental conditions to provide more detailed insight into hazard characteristics (e.g., ranges of floodwater depths, wave action, extent of storm surge above flood boundaries), as well as knowledge of existing flood mitigation measures in place at potentially affected facilities.

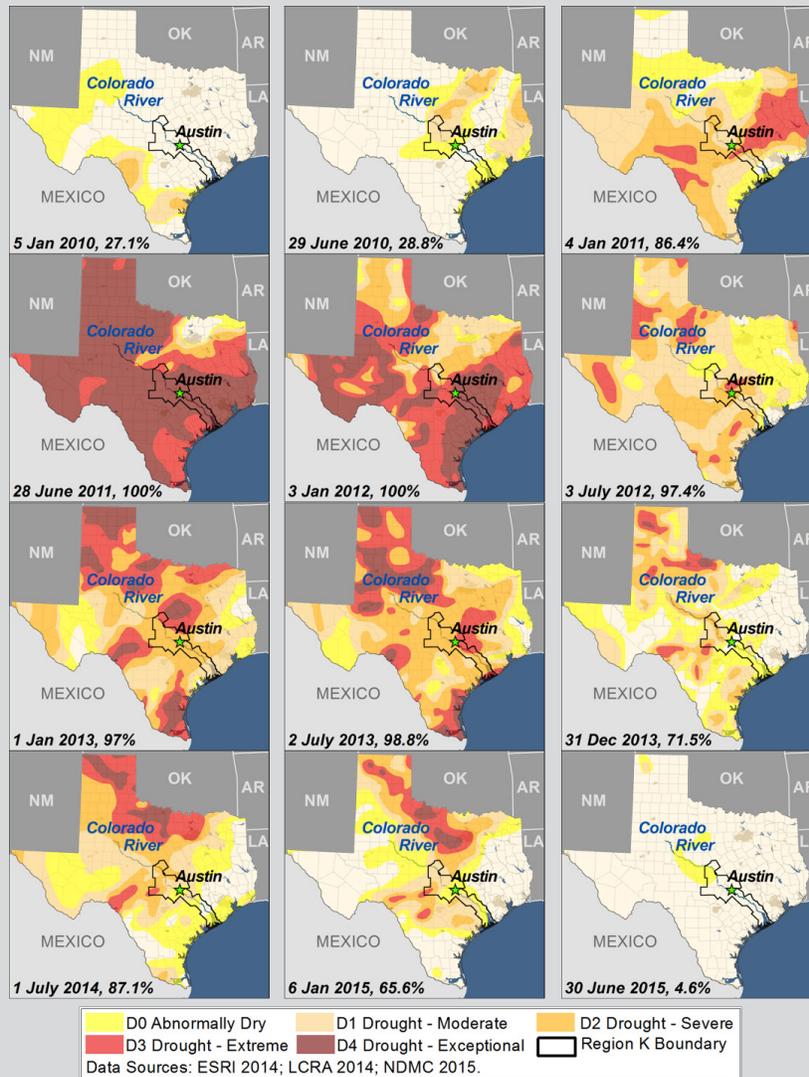


An RRAP project focused on the resilience of transportation infrastructure in Jacksonville, Florida, included a hurricane impact analysis. Located on the banks of the St. Johns River just upriver from the Atlantic Ocean, Jacksonville is a major transportation hub in North Florida with regionally and nationally significant transportation infrastructure. The geography of Jacksonville is well-configured for international supply-chain operations with easily accessible ports, airports, railways, and interstate highways. The proximity to the Atlantic Ocean, St. Johns River, and the Intracoastal Waterway (Nassau River) also makes the Jacksonville area vulnerable to hurricanes, tropical storms, and the effects of coastal and inland flooding. Therefore, a key focus of the project was identifying the vulnerability and consequences associated with a devastating Category 3 hurricane affecting the Port and other infrastructure assets in the Transportation Sector. Even though a hurricane of that magnitude is relatively rare in Jacksonville, nevertheless in 2017 Hurricane Irma made landfall in Florida as a Category 4 storm and then produced record flooding in Jacksonville. (CISA, *Resiliency Assessment: Jacksonville Transportation*. May, 2016.)





An RRAP project focused on the impact of a prolonged drought in Texas on the Lower Colorado River basin and related infrastructure interdependencies (i.e., water, wastewater, and energy). During the drought, a number of Texas communities were threatened with the loss of local water sources, and a few electric generation facilities faced the possibility of shutdown because of the potential loss of water for cooling. The project team leveraged information from the U.S. Drought Monitor, which synthesizes various drought indices and impacts and represents a consensus view of academic and federal scientists about ongoing drought conditions. A summary visual showed the progression of drought conditions in Texas at 6-month intervals from January 2010 through June 2015. Between March 2011 and January 2012, nearly 100 percent of Texas was in some form of drought. During June through November 2011, 65 percent or more of Texas was in “exceptional” drought, the most severe level. A finding from the project concluded that long-term water and electricity planning does not consider the potential impacts on precipitation and temperature from future environmental states, such as increased temperatures and seasonal changes in precipitation, which can exacerbate drought conditions. (CISA, *Resiliency Assessment: Central Texas Drought*. August, 2016.)



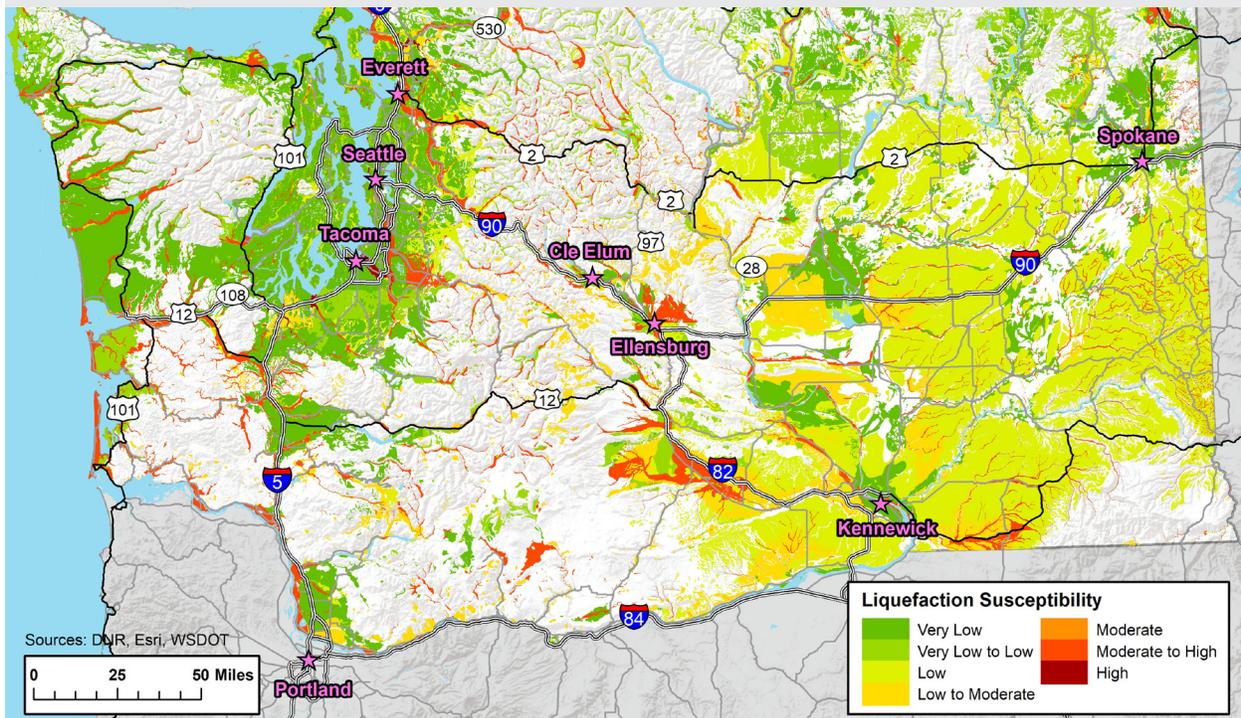
## Vulnerability Analysis

A vulnerability is a physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.<sup>43</sup> Thus, in order to evaluate vulnerabilities for a given infrastructure, identifying one or more relevant threats or hazards is an important step in assessing the infrastructure’s security or resilience posture. Assessments focused on understanding the consequences of disruptions inherently incorporate vulnerability analysis,

as their objective is to understand the impact of a specific threat or hazard on a certain system or set of infrastructure. Assessments focused on characterizing one or more infrastructure systems likely also address vulnerabilities, but it typically occurs at a more general level, focusing more on the identification of potential vulnerabilities rather than specific analysis of how vulnerable a specific asset or system is or the potential consequence of that vulnerability’s exploitation.



An RRAP project explored the resilience of surface transportation in the State of Washington, seeking to understand the vulnerability of roads and bridges in the state infrastructure to a Cascadia Subduction Zone earthquake. One secondary hazard arising from earthquakes is soil liquefaction, which refers to the phenomenon where soils that are saturated with water can behave like a liquid when they experience seismic shaking. CISA leveraged a statewide geospatial database maintain by the Washington Department of Natural Resources that characterizes soil liquefaction susceptibility in the top-most layer of soil across the state, shown below. This dataset served as the primary basis for analyzing seismic-related ground failure impacts to the statewide transportation system in Washington State. (CISA, *Resiliency Assessment: Washington State Transportation Systems*. March, 2019.)



<sup>43</sup> DHS, *DHS Risk Lexicon: 2010 Edition*. September, 2010. Accessed February 13, 2020. [www.cisa.gov/dhs-risk-lexicon](http://www.cisa.gov/dhs-risk-lexicon).

## Criticality Analysis

Criticality analysis involves qualitatively or quantitatively assessing the relative importance of infrastructure assets to a mission or function, or continuity of operations.<sup>44</sup> Assets are compared to other assets within an infrastructure system based on common criteria or attributes to identify the relative importance of specific assets within the infrastructure system. Assets can be point assets at a single location (e.g., electric power substation or natural gas city gate) or distributed assets spanning a larger geographic area (e.g., electric power transmission line or water main). In network analysis, point and distributed assets are known as nodes and links or edges, respectively. (See the Network Analysis section for more information.)

Effective criticality analysis requires identification of specific attributes for comparison. These attributes typically focus on one or more key properties of the infrastructure asset (e.g., connectivity within an infrastructure system, commodity flow through the asset, utilization factors to understand capability to handle increased demand). Also important is a determination of whether to evaluate asset criticality based on steady-state operations (i.e., “blue sky” scenarios) or disrupted operations (i.e., “grey sky” scenarios with partial or short-term disruptions, or “black sky” scenarios with extensive, long-term disruptions). These analyses can explore commodity flows through specific assets within disruption scenarios and the potential for assets to serve additional demand. They can also be used to compare performance of assets during normal and disrupted conditions. Aggregating results from criticality analysis across multiple infrastructure systems can help regional partners identify geographic locations where critical assets are highly concentrated. These clusters may be candidates for more detailed system-level analysis, mitigation investments, or future infrastructure planning efforts.

## Comparative Analysis

Comparative analysis is an essential component of criticality analysis, but has other applications when performing regional infrastructure resilience analysis. Analytic questions that customers pose often center on trying to understand what infrastructure is most at risk, least prepared, or most vulnerable. All of these questions include an implied comparison of some infrastructure attribute or combination thereof (e.g., location, vulnerability, consequence). The tools and techniques used to perform comparative analysis will vary widely depending on the nature of the questions to be answered and attributes used for comparison. All comparative analysis demands consistent data elements, which should drive data collection to use standardized question sets or assessments as much as possible in order to reliably produce the same data points every time. An important consideration for any comparative analysis is the early identification of appropriate attributes for comparison that will answer the analytic question. Statements like “most vulnerable” or “highest risk” must be decomposed and the attributes that would indicate such factors need to be identified before an appropriate approach can be developed to collect the required data for comparison. Comparative analysis is integral to decisions associated with prioritization (e.g., risk-informed decision making), and thus a common and important demand from stakeholders seeking insight into how to allocate limited resources to achieve the greatest resilience effect.

<sup>44</sup> CISA, *DHS Risk Lexicon: 2010 Edition*. September, 2010. Accessed February 13, 2020. [www.cisa.gov/dhs-risk-lexicon](http://www.cisa.gov/dhs-risk-lexicon).

## Geospatial Analysis

The analysis of regional resilience relies heavily on sound geospatial data. Geographically based sources of information provide an analytically defensible and visually compelling basis for decision making. This has led to the increased use of geographic information system (GIS) software, including proprietary applications (e.g., ESRI's ArcGIS) and open-source options (e.g., QGIS). Planning as a profession is accustomed to working with large complex data sets and to using GIS and similar software to model various phenomena and to analyze scenarios. Examples of urban modeling software include Community Viz, What If? and UrbanSim. Having access to local land use, building, and development data and technical resources can be crucial to prevention, preparedness, mitigation, response, and recovery activities. However, anecdotal evidence suggests that planners and first responders do face challenges in exchanging data and information, whether in day-to-day transactions or in crisis situations. Reliance on technologies such as GIS, GPS, and related planning information systems is growing rapidly in local jurisdictions across the United

States and are considered vital tools in crisis management.<sup>45</sup> Similarly, they are increasingly valuable for resilience analysis as they allow users to orient infrastructure systems spatially and visualize disruption scenarios based on how these systems operate.

Geospatial analysis refers to the use of geospatial information and visualization tools to model or create mathematical representations of real-world systems for the purpose of studying their behavior and improving their design.<sup>46</sup> Regional planners, for example, often model future development and estimate its economic, environmental, and social outcomes under alternative planning scenarios. Transportation planning and travel demand models predict changes in travel patterns and the demands on a transportation system that occur in response to changing regional demographics, land use and development patterns, and transportation infrastructure. Improvements in the collection, processing, sharing and protection of national geospatial information is enhancing the availability of common data sets that in turn drive enhanced geospatial visualization and analysis. A number of government agencies are making GIS data sources available for wide use.



<sup>45</sup> American Planning Association, "APA Policy Guide on Security." 2005. Accessed February 13, 2020. [www.planning.org/policy/guides/adopted/security.htm](http://www.planning.org/policy/guides/adopted/security.htm).

<sup>46</sup> CommunityViz, *CommunityViz in Transportation Planning and Modeling*. Undated. Accessed February 13, 2020. [www.communityviz.city-explained.com/PDFs/articles/WhitePaperTranspModeling.pdf](http://www.communityviz.city-explained.com/PDFs/articles/WhitePaperTranspModeling.pdf).



## Accessing Available Geospatial Data

Improvements in the collection, processing, sharing and protection of national geospatial information across multiple levels of government is helping to provide a common foundation for data visualization and analysis. Examples include the following:

- The HIFLD Subcommittee Online Community hosts an open-data portal containing national foundation-level geospatial critical infrastructure data. It contains 320 public datasets that consist of re-hosted public data and direct pointers to live data services.
- The U.S. DOT Bureau of Transportation Statistics develops geospatial information and visualization tools, conducts spatial and network analyses, develops performance measures related to the transportation network and geographic accessibility provided by the network, prepares maps, coordinates the transportation layer of the National Spatial Data Infrastructure, and publishes the National Transportation Atlas Database.
- The U.S. DOT National Pipeline Mapping System (NPMS) provides a public map viewer that enables the user to view NPMS pipeline, liquefied natural gas plant and breakout tank data one county at a time, including attributes and pipeline operator contact information. Users can also view gas transmission and hazardous liquid pipeline accidents and incidents going back to 2002 for the entire United States.
- The USCG collects real-time vessel data in the Automatic Identification System, which provides location, destination, sailing draft, and vessel speed data over time as vessels move. Additional data include the ship name, classification, call sign, registration number, as well as maneuvering information, closest point of approach, time to closest point of approach, and other navigation information.

## System Diagramming

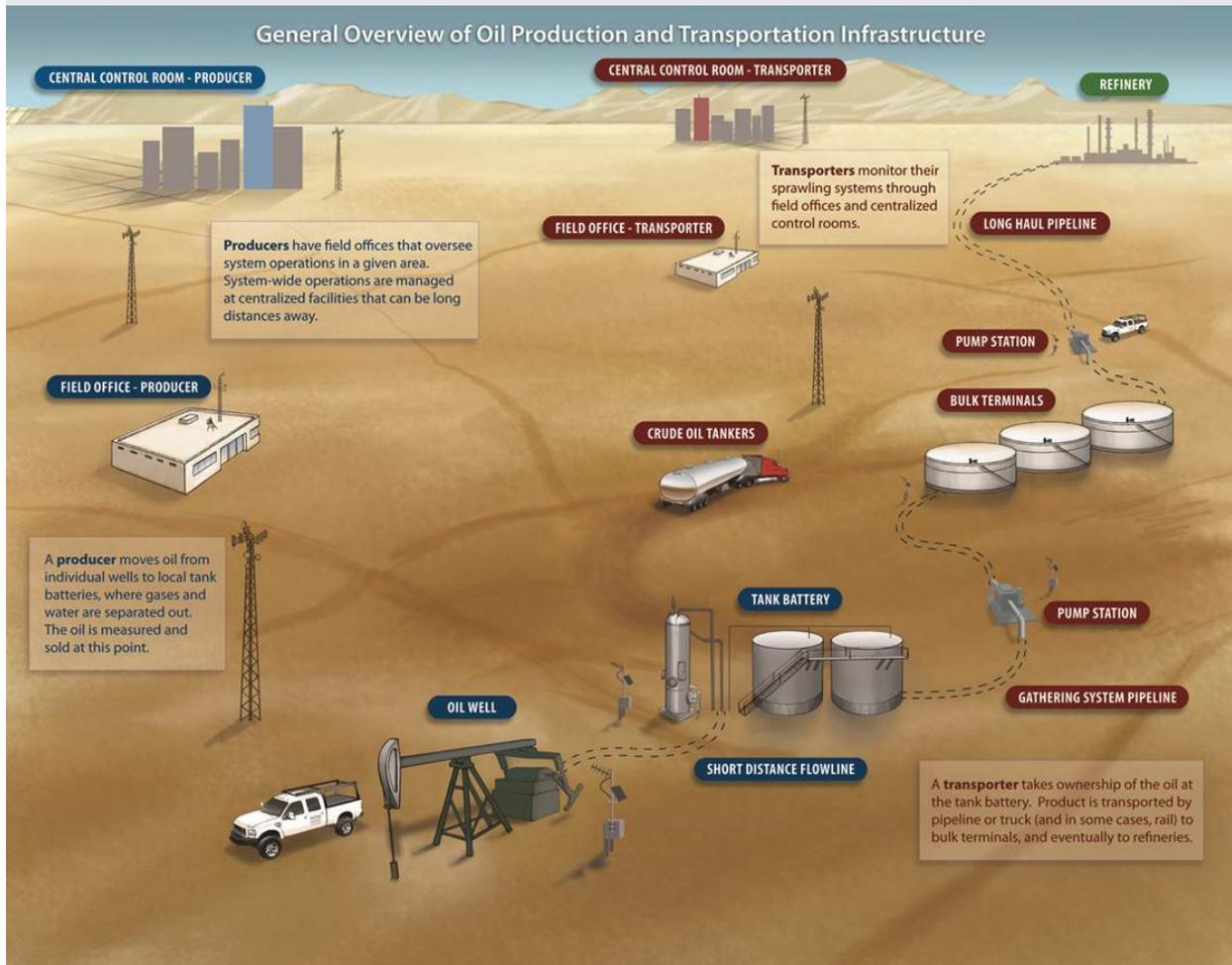
A system diagram is the visualization of the components of a system and the connections (logical or physical) among them that define how the system operates. These diagrams can be basic illustrations of essential inputs and outputs, or more complicated visuals reflecting potential avenues for disruption. System diagramming is a useful output from infrastructure system analysis, capturing a high-level overview of key system dynamics in an approachable visual format. This approach enables identification of single points of failure and more critical nodes within the infrastructure systems. Steps to consider in the system diagramming process are mapping how the system works under normal operations; identifying what upstream and downstream entities depend on the system; documenting what inputs are required for certain components of the system to operate; and identifying what factors could adversely affect the operation of specific components and the system as a whole.

System diagrams are helpful for conveying the significant components of an infrastructure system to ensure entities involved in planning efforts understand the complexity of the infrastructure systems involved. They can also inform processes to prioritize assets and subsystems for expanded or more detailed analysis, as well as provide a helpful basis for performing failure analysis by identifying key components and functions within the system. System diagrams may also be abstracted to highlight flows of goods through a system, focusing less on individual assets and instead characterizing the overall inputs to and outputs from a system. Diagramming not only helps document the infrastructure components and how they operate, but also can inform briefings to external parties about the assessment. They may even form the basis of final graphics for the assessment that depict the system.





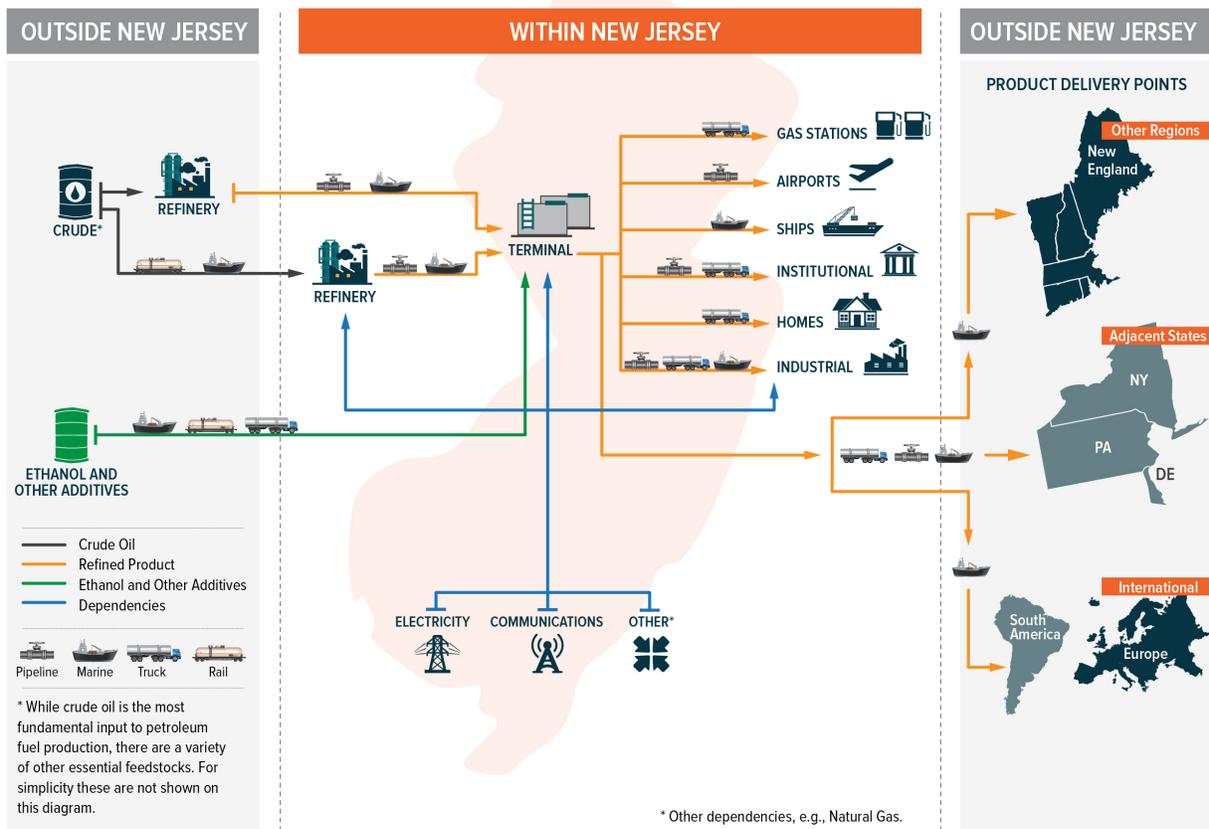
An RRAP project focused on the use of SCADA systems for crude oil production and transportation in the Permian Basin region of West Texas, and corresponding security concerns. This region is the Nation’s top source of oil, accounting for over 20 percent of U.S. production. The project examined the important role of SCADA, factors that can increase system vulnerabilities, and the types of impacts that could arise from a successful attack on SCADA systems. A worst-case cyber-attack scenario could entail major disruptions to Permian Basin operations and cause cascading effects that extend well beyond Texas. As part of the project, various aspects of the crude oil production and transportation process in the Permian Basin were developed, identifying connections among oil production and transportation infrastructure, communications links, and potential points of cybersecurity concern. The diagrams provide a general understanding of how the integrated oil and transportation systems are and where communications and cybersecurity considerations can come into play. (CISA, *Resiliency Assessment: Permian Basin*. June, 2016.)





The infographic below illustrates that New Jersey’s fuel supply chain not only transports finished petroleum products throughout the state itself, but also to customers in neighboring states (New York, Pennsylvania, and Delaware), different regions (New England), and even to different continents. (CISA, *Resiliency Assessment: New Jersey Petroleum*. April, 2015.)

### PETROLEUM MOVEMENTS THROUGH NEW JERSEY



## Capability Analysis

A capability is defined as the means to accomplish a mission, function, or objective.<sup>47</sup> Capability analysis centers on identifying specific capabilities required to address a given threat or hazard, or the consequences thereof, in terms of planning, organization, training, equipment, and exercise elements and then evaluating readiness to deliver those capabilities when requested in a timely manner. As illustrated by its alignment with preparedness, infrastructure resilience is a function of both the physical design and engineering of the infrastructure and the capabilities of the organizations involved in its operation. Well-developed capabilities can help mitigate existing infrastructure vulnerabilities and lessen the consequence of disruptions or damage through things like alternate operating procedures, well-practiced rapid response protocols, stockpiling and pre-positioning of critical supplies and parts, and backup capacities. For the purposes of regional resilience analysis, it is important to analyze the capabilities of not only the infrastructure operators, but also other regional organizations involved in incident management. These outside organizations (e.g., transportation agencies, emergency management offices, and mutual aid partners) have various capabilities that can be leveraged to mitigate impacts to and consequences of an event affecting infrastructure, thus contributing to its overall resilience. Examples include capabilities such as directing electric power restoration priorities; supporting roadway clearance and debris removal; controlling access to affected areas; providing emergency equipment (e.g., electric generators); and expanding access to utility crews or spare parts.

## Plans Analysis

Within a given region, multiple plans likely exist to guide steady-state and emergency activities for local, state, and federal partners. Steady-state plans may articulate day-to-day roles and responsibilities for particular agencies and the capabilities they bring to bear to accomplish them. Emergency operations plans typically outline planning assumptions that set the

context for response efforts and define roles and responsibilities for relevant partners to respond to various hazards and return to normal operations. A comparative review of these operational plans from regional partners can surface capability gaps and incomplete planning assumptions that may be relevant to assessing infrastructure resilience. Issues to watch for in these reviews are cases where plans do not appear to account for the consequences arising from an infrastructure disruption that is likely to occur in a given scenario; reflect incorrect assumptions about how particular infrastructure systems will perform under different conditions described in the plans; or conflict with one another about roles and responsibilities associated with infrastructure operations. Parallel reviews of planning documentation that governs land use, the design and operation of civic space, utility networks, transportation systems, and other public facilities may surface additional issues.



An RRAP project assessed the resilience of the City of Fort Collins, Colorado, with a goal of determining resilience gaps for social institutions (i.e., community service organizations, education, government, and healthcare) and lifeline infrastructure systems (water, energy, transportation, and communications) that support them relative to a catalog of specific hazards. As part of the project, CISA reviewed and analyzed over two dozen city, county, and state plans to identify gaps in infrastructure and infrastructure-resilience concepts within and across plans, with an eye toward evaluating how the jurisdiction plans to ensure the resilience and security of key social institutions and supporting lifeline infrastructure systems within its control. The plans were relevant to establishing recovery time objectives for key systems. (CISA, *Resiliency Assessment: Fort Collins*. November, 2018.)

<sup>47</sup> DHS, *DHS Risk Lexicon: 2010 Edition*. September, 2010. Accessed February 13, 2020. [www.cisa.gov/dhs-risk-lexicon](http://www.cisa.gov/dhs-risk-lexicon).

## Data Aggregation

Data aggregation is a statistical process of combining disaggregated data (i.e., data with multiple parameters) in order to identify specific trends indicated in the data for one or more parameters. Data aggregation is important for extracting summary statistics, identifying trends, and visualizing them effectively. Data aggregation is particularly relevant for large data sets that are housed in one or more complex databases. The process of aggregating data points of interest sacrifices some data detail in favor of enhanced clarity and usability for a broader audience. Data aggregation is a core feature of the emerging field of data science, which integrates scientific methods, computer science, and mathematics in order to mine extremely large and complex data sets and generate information in new formats and structures that produce useful and actionable insights for decision makers.

An example of data aggregation is extracting trends information in a large database containing infrastructure assessment data and using that to explore vulnerability to future extreme weather events. In this case, vulnerabilities of infrastructure to various climate change variables (e.g., in the electric power, natural gas, and petroleum subsectors) are aggregated to show the vulnerabilities of energy infrastructure to all climate change by likelihood of occurrence and projected magnitude of impact. This aggregation process would enable the identification of high-risk climate change variables, impacts, key dependencies, and potential resilience measures for each of the energy subsectors, as well as cross-sector trends.



An RRAP project provided a cross-sector review of New York City energy, transportation, and communications infrastructure at risk from future extreme weather events. The project capitalized on New York City infrastructure risk data collected by the Mayor's Office of Recovery and Resiliency to identify vulnerabilities, including dependencies and interdependences that amplify system risk and high-consequence failure points that could result from future extreme weather events. As part of this project, CISA analyzed responses from infrastructure owners and operators in New York City to a questionnaire from the city's Climate Change Adaptation Task Force, augmenting that data with national-level CISA infrastructure asset assessment data. This process enabled the identification of high-risk climate change variables, impacts, key dependencies, and potential resilience measures for key infrastructure sectors, as well as cross-sector trends. (CISA, *Resiliency Assessment: New York City Energy, Transportation, and Communications*. March, 2019.)



## Network Analysis

A network is a system of interconnected elements that represent possible paths from one location to another. Network analysis is used in a wide range of disciplines, including epidemiology, mathematics, computer science, electrical engineering, transportation planning, project management, organizational design, and complex systems analysis, to name a few. Diagrams of physical and virtual networks are used to visualize key elements in a system or process, understand patterns of activity and relationships, identify critical paths to success, and flag potential failure points. Even a simple network diagram—with general indicators for key nodes and links and without key data points for infrastructure on physical location, capacity, volume, speed, or cargo type—can be an illuminating contribution to infrastructure assessments, allowing analysts to identify key clusters of activity, high-level vulnerabilities, and potential consequences of disruption.

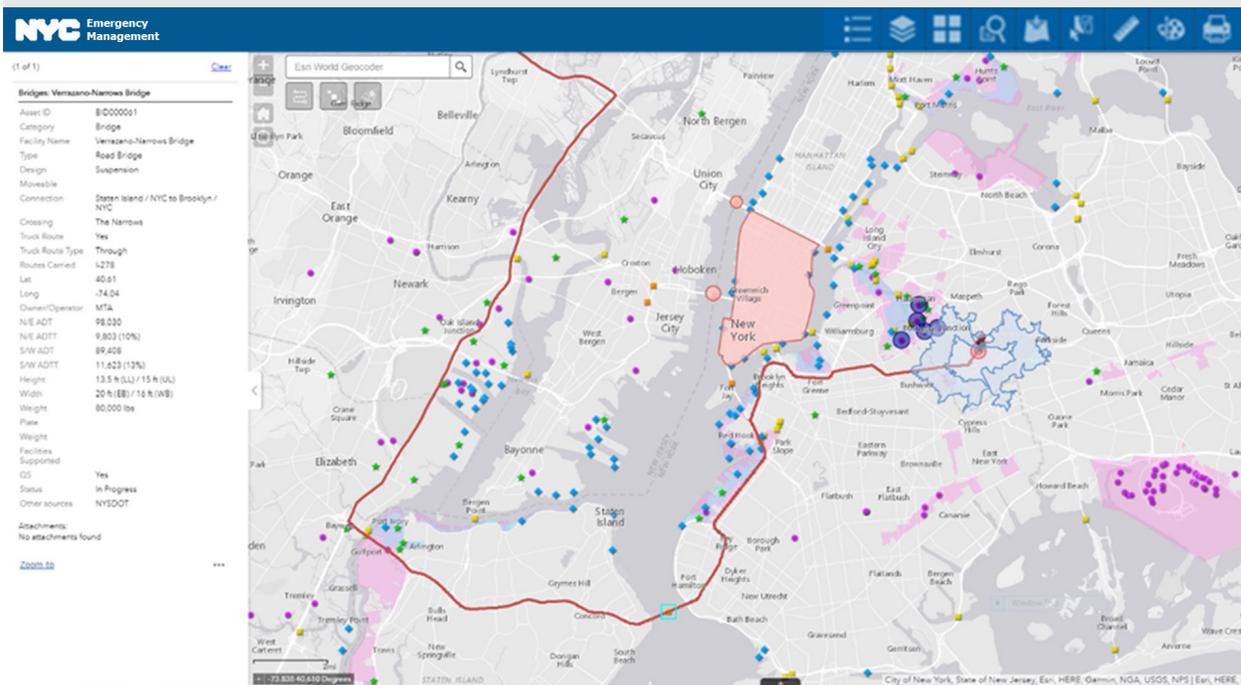
In the infrastructure domain, people, resources, and goods tend to travel along networks: vehicles travel on roads, airliners fly on predetermined flight paths, oil flows in pipelines. By documenting and modeling potential paths within a network, analyses related to the movement of the vehicles, oil, or other agents on the network becomes possible. Network analysis is an especially important tool in understanding infrastructure dependencies and interdependencies, where analysts explore upstream and downstream connections across multiple infrastructure systems. Key questions explored in dependency analysis (i.e., what resource is needed and why? Who provides it? Where does it come from? How is it provided? When is it provided?) lend themselves to network analysis, in both a generalized way and more detailed layouts that harness real-world geospatial and technical features.

Network analysis is a valuable mechanism for understanding and documenting relationships within and among systems. In addition to establishing a baseline characterization of a given network, a common focus of network analysis is finding the shortest path between two points, recognizing that the shortest route could reflect different variables, such as distance, time, and money. Network analysis can also shed light on how goods, services, information, or people flow through a network, which nodes and links are central to its operations, and how many possible paths exist. In addition to understanding how physical systems operate, network analysis can also be applied to social structures to understand and test how individual actors relate to one another and how information circulates. This application can support evaluation of logical dependencies and other network considerations that stretch beyond the physical features of how infrastructure systems operate in steady-state and crisis operations.

Physical networks can include geometric networks that allow travel in only one direction at a time (e.g., rivers or electrical, gas, sewer, and water lines). The agent in the network—for instance, the oil flowing in a pipeline—cannot choose which direction to travel; rather, the path it takes is determined by external forces (e.g., gravity, electromagnetism, water pressure). An engineer can control the flow of the agent by controlling how external forces act on the agent. Transportation networks allow travel in both directions through surface, maritime, or air domains. The agent on the network—for instance, a truck driver traveling on roads—is generally free to decide the direction and destination. A network dataset can model a single mode of transportation, like roads, or a multimodal network made up of several transportation modes including roads, railroads, and waterways with multimodal interconnects (e.g., terminals).



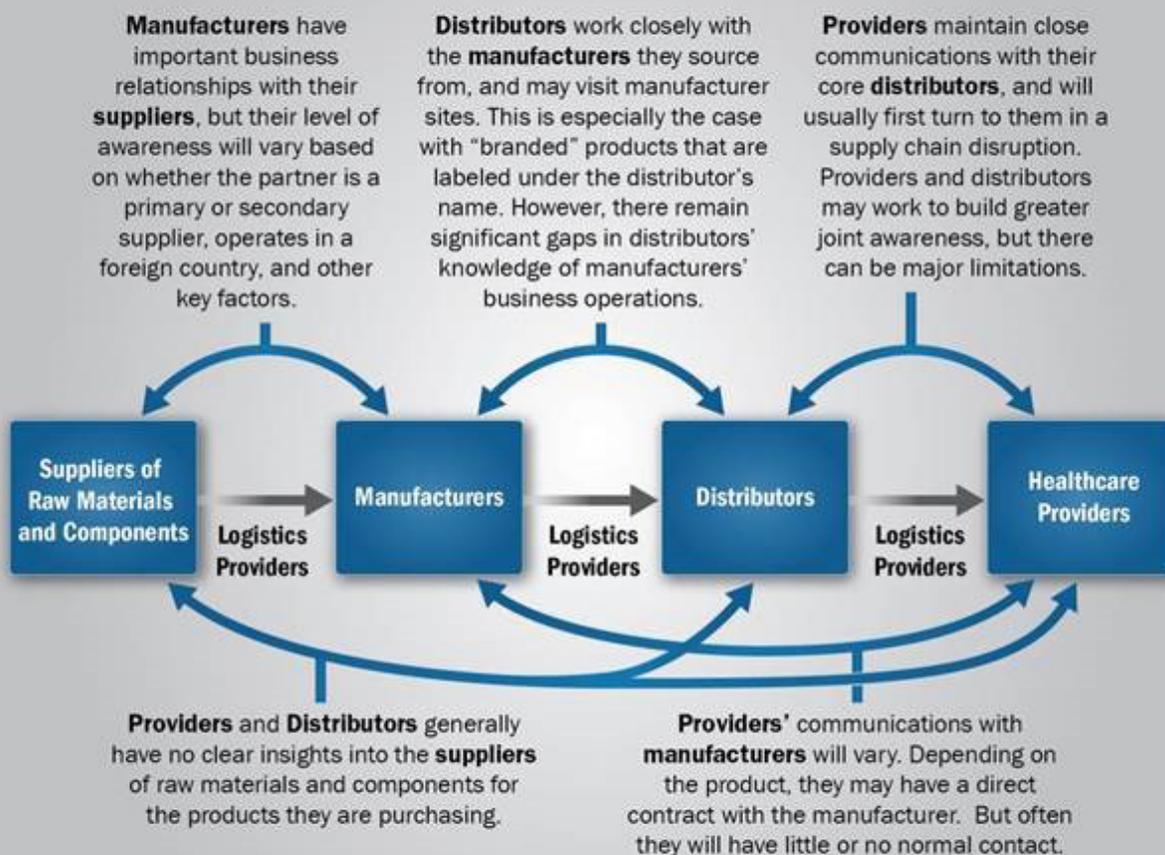
An RRAP project focused on critical supply chains in New York City involved the development of a multimodal freight transportation network that reroutes freight movements around disruption areas and between road, rail, and maritime transportation links and nodes. Assessments of the exchange capabilities at intermodal facilities, time requirements for exchanges, and congestion along corridors were considered in determining which primary or alternative routes would be the most efficient. The results are used by NYC Emergency Management to forecast how the freight network could absorb or adapt to disruptions, and deliver critical supplies to those in need. (CISA, *Resiliency Assessment: New York City Critical Supply Chains*. November, 2018.)





An RRAP project explored regional concerns about healthcare supply chains in the New York City area. The goals were to help build the groundwork for a stronger and more coordinated focus in the region on significant risks to healthcare supply chains, and to identify opportunities in the region to individually and collectively implement long-term resilience strategies that minimize impacts to patient care due to supply-chain disruptions. The project concentrated on five categories of healthcare products: medical-surgical items; pharmaceuticals; blood products; medical gases; and linens. Through this effort, CISA developed a series of supply-chain profiles that present important attributes and risk considerations for each of these categories. In addition, CISA created a document that breaks down many of the key factors that define healthcare supply-chain disruption events, along with considerations for several scenarios that could impact the supply chains serving the region. (CISA, *Resiliency Assessment: New York City Regional Healthcare Supply Chain*. October, 2018.)

### Cross-Organizational Awareness in Healthcare Supply Chains



Information awareness can also be crucial for other organizations, such as logistics providers and other supply chain service companies, group purchasing organizations, and government agencies.

## Failure Analysis

Protecting critical infrastructure, especially in a complex urban area or region, should focus on identifying and prioritizing potential failure points that would have the most severe consequences. Such prioritization can inform targeted planning and investment decisions, such as what infrastructure should be hardened or relocated first or what infrastructure should receive priority restoration following a disaster, among other uses. Without a prioritization process, assessment and protection programs are typically guided by intuition or expert judgement, and they often do not consider system-level resilience. While understanding how to prioritize high-consequence failure points for assessments and, for protection is essential, the complexity of infrastructure systems can quickly overwhelm.

A fundamental component of critical infrastructure security and resilience programs should include understanding how, why, and where systems fail. This understanding should guide decisions on where to conduct in-depth assessments as well as which protection and mitigation measures to pursue. However, a complicating factor is that infrastructure failures vary significantly. Some failures will generate significant consequences at the system or regional level, whereas effects from other failures remain local, while still others have little to no effect on the overall service provided.

Fault tree analysis is an example of one specific approach for failure analysis that is used widely in engineering (e.g., nuclear, aerospace) in conjunction with event trees. In this deductive approach, analysts specify an undesired state of the system (often a state that is important from a safety standpoint) and then analyze the system in the context of its environment and operations to find all credible ways in which the undesired event can occur. Fault tree analysis does not try to identify or understand all possible system failures. Rather, users identify at the highest level how a system has failed (e.g., plane crash) and then explore how that scenario could have occurred. The results of fault tree analysis are therefore bound by the failure scenarios that stakeholders have elected to explore.<sup>48</sup>



## Using Modeling Effectively

Modeling can be a powerful tool in regional assessments of infrastructure, but it can also introduce potential misunderstandings about the results that it generates and ways to use those results. Models are not a perfect replication of how a particular system operates, due to data availability, inherent operational uncertainty, information security, or omission of human factors. Thus, in real-world operations, performance will likely differ from simulations generated through modeling. However, models allow analysts to experiment with approximations of how systems will operate under a specific set of simulated present or future conditions. Modeling can help users identify critical nodes and potential failure points that merit further attention with system operators and regional planning communities. Of particular value are models that have undergone third-party validation and peer review, which introduces greater confidence in the results that they generate.

<sup>48</sup> Vesely, W.E., F.F. Goldberg, N.H. Roberts, and D.F. Haasl, *Fault Tree Handbook* U.S. Nuclear Regulatory Commission, NUREG-0492 (Washington, DC: U.S. Government Printing Office, 1981).

## Modeling and Simulation

Models can inform regional assessments of infrastructure by allowing users to explore and simulate how various entities—including infrastructure systems, organizations, and people—would react under certain conditions. These tools can help users identify critical failure points in infrastructure systems that could trigger significant downstream impacts; they can also assist users in exploring human and organizational decisions. However, it is important to recognize that these models are not intended to provide exact replications of system performance. Rather, they can serve as valuable screening tools to help identify critical nodes, allowing assessment teams to dedicate limited resources to areas of relatively greater concern.

Modeling employed for critical infrastructure resilience analysis is usually addressed from two perspectives: by infrastructure system and by threat or hazard. Infrastructure system models often focus on a single type of system (e.g., electric power, natural gas, petroleum, water, transportation). This makes the problem manageable by breaking the infrastructure down into its individual sectors and subsectors (e.g., electric power models have been developed to model the electric grid, water models to model water infrastructure). These tools enable users to see how a given system reacts when one or more critical nodes is disrupted. The threat and hazard perspective focuses on understanding how these phenomena (e.g., hurricanes, earthquakes, cyber attacks, climate change) could manifest or behave

to disrupt infrastructure system operations. These two types of models can be coupled in order to assess how a certain hazard is likely to affect an infrastructure system. For example, a model of coastal flooding conditions can be combined with a model of the electric power system to understand how the loss of electric system components due to flooding will affect the delivery of electric power.

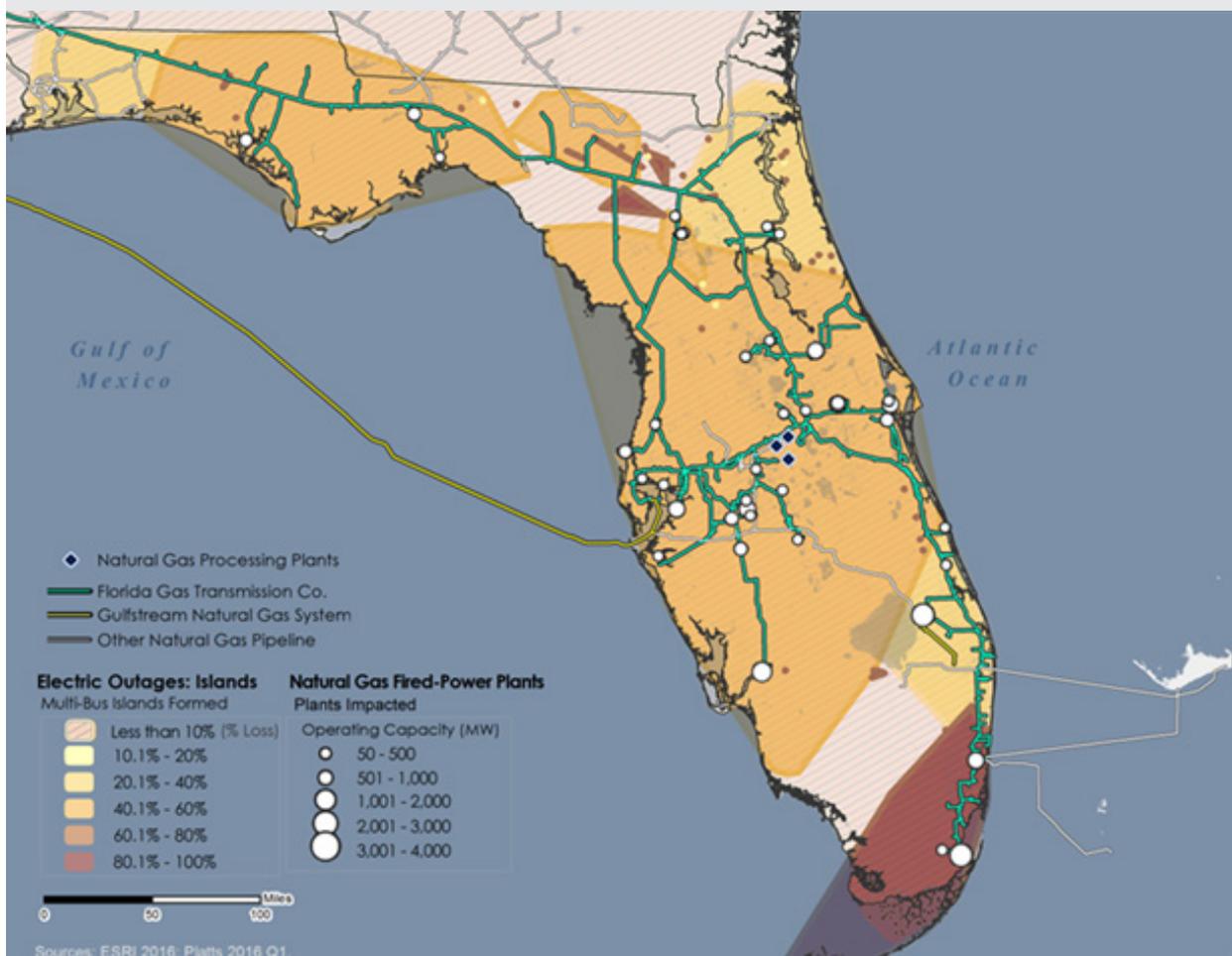
Agent-based modeling is another simulation method that involves independent agents making decisions and taking actions based on individual goals and priorities within an environment. Agents react to external stimuli from other agents and from the environment, which in turn may be affected by the agent decisions. Agent-based modeling is an ideal methodology for assessing the changes driven by the choices of a population that is hard to estimate directly. Agents can be active, making decisions and engaging other agents (e.g., utilities) to achieve goals, or passive, responding to other agents or the environment (e.g., regulatory agents).

Modeling is also a feature in more advanced geospatial analysis, in which a simulation platform can create maps and scenarios that in turn feed an external model for numerically intensive calculations and ingest results for display and further analysis. External models can be implemented in different platforms that use inputs from databases, geodatabases (GIS maps), or tables. Example geospatial modeling related to infrastructure could include travel demand models, water runoff, and energy use.



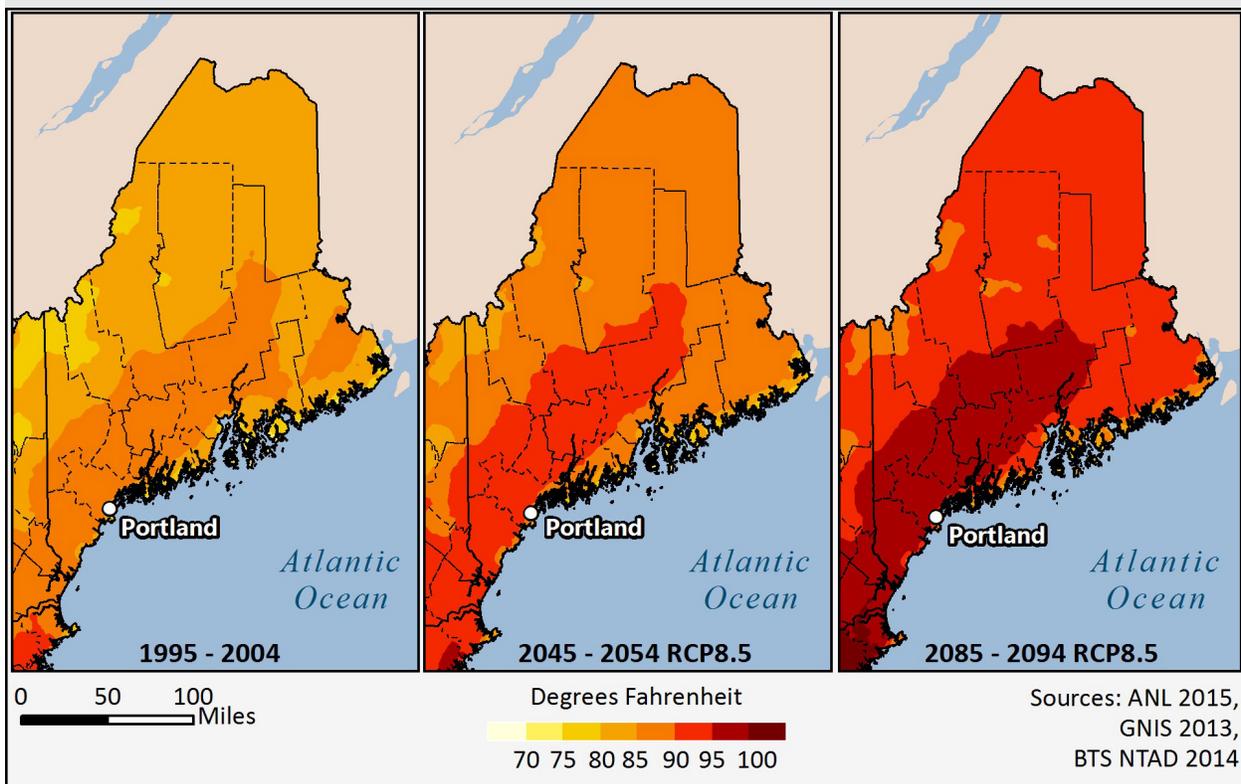


No significant oil production facilities or refineries exist in Florida, so all petroleum products must be transported into the state. A recent RRAP project focused on improving state and local understanding of the complex petroleum fuel supply chain serving the state. The project also helped state and local planners identify vulnerabilities throughout the petroleum fuel supply chain and develop a realistic strategy designed to mitigate and manage a large-scale failure of petroleum-related port operations. One case study related to the project used energy system modeling to illustrate the dependences between natural gas and electric power. In this scenario, a complete break on a major interstate transmission pipeline supplying natural gas to the state results in a 100 percent reduction in the flow of gas through the pipeline. The pipeline break also disrupts fuel delivery to a large number of gas-fired power plants. As a result, electric power generation would be affected, leading to potential disruptions across the state with varying load loss intensity ranging from 10-100 percent. (Portante, Edgar, Brian Craig, James Kavicky, Leah Talaber, and Stephen Folga, "Modeling Electric Power and Natural Gas Systems Interdependencies," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, Washington, D.C., USA, May–June, 2016. Accessed February 13, 2020. [https://cip.gmu.edu/2016/06/03/modeling-electric-power-natural-gas-systems-interdependencies/.](https://cip.gmu.edu/2016/06/03/modeling-electric-power-natural-gas-systems-interdependencies/))





An RRAP project in Maine focused on the local and regional consequences of climate disruptions and their impacts on critical infrastructure in the Casco Bay Region, the most developed and populous region in Maine. As part of this process, the project team conducted a detailed hazard analysis—which involved developing climate projections for the Casco Bay Region based on global climate models, which are dynamically downscaled using a regional climate model. The team then used those results to prioritize and inform related dependency analyses on specific infrastructure systems. For example, the team performed an assessment of the vulnerability of key substations to characterize the resilience of the regional electrical power system to potential future flooding and storm impacts under climate change. This substation case study considered historical and projected changes in average and extreme precipitation, sea-level rise, and storm surge that were then used to define two disruption scenarios. (CISA, *Resiliency Assessment: Casco Bay*. March, 2016.)



## Decision Analysis

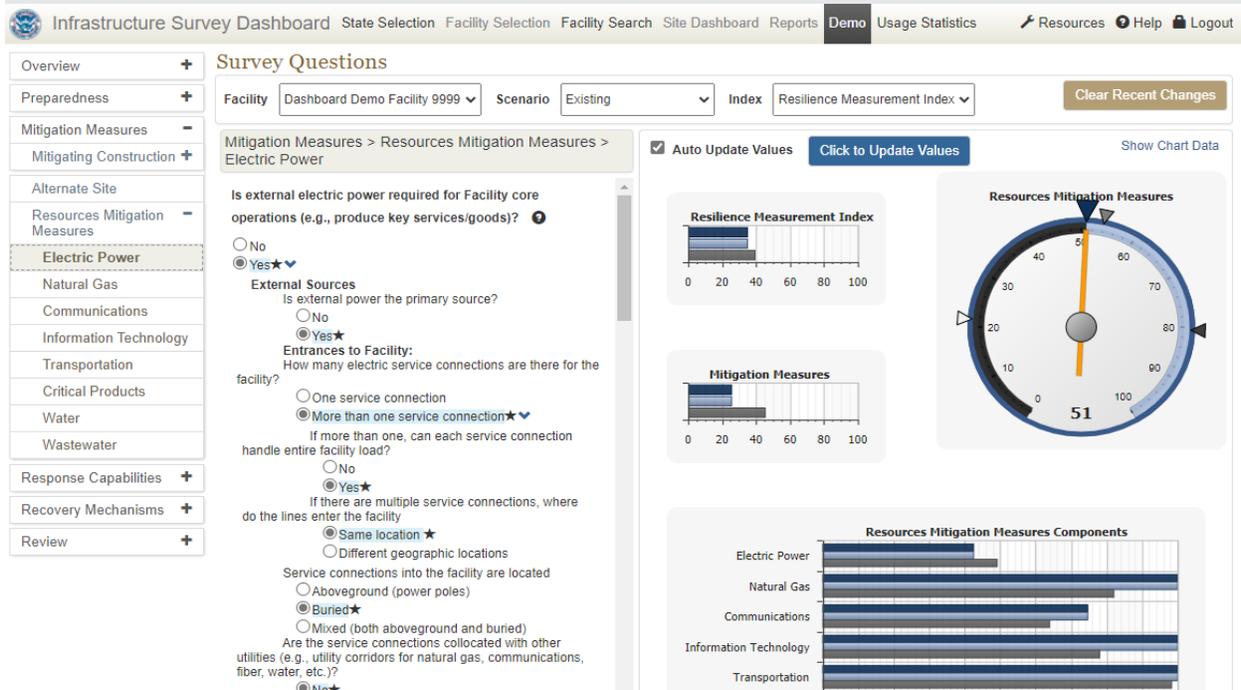
Decision analysis is a systematic and logical set of procedures for analyzing complex, multiple-objective (multi-criteria) decision problems. It uses a “divide and conquer” philosophy in which hard-to-define, high-level objectives are successively divided into lower-level objectives that are more easily understood, defined, and evaluated. Practitioners use decision analysis to develop meaningful measurement scales for objectives, examine trade-offs among conflicting objectives, and incorporate uncertainty and risk attitudes as appropriate. Ultimately, decision analysis provides a formal, systematic way to identify key elements of a decision, understand the relative implications

of tradeoffs, and identify courses of action that achieve desired outcomes.

Decision analysis is an interdisciplinary field that brings together economics, mathematics, psychology, and management. It is used widely in business, healthcare, environmental sciences, energy exploration, and public policy, among others, to understand risk and strategies for managing it. Decision analysis includes models for decision-making under conditions of uncertainty or multiple objectives; techniques for risk analysis; economic analysis of competitive and strategic decisions; techniques for facilitating group decision-making; and computer modeling software and expert systems for decision support.<sup>49</sup>



In the infrastructure resilience space, decision analysis has been useful for developing approaches to measure resilience. For example, the Resilience Measurement Index that CISA uses in its assessment process for individual infrastructure assets reflects the relative importance of each characteristic that contributes to the overall resilience of a facility. The various resilience factors accounted for in that index are drawn from a set of questions used in a CISA infrastructure assessment and reflect weights of how important each factor is to resilience based on results of a formal elicitation process with subject matter experts from government and industry. Other applications include using decision analysis techniques to objectively compare different options for improving resilience at an infrastructure facility or system.



<sup>49</sup> Financial Times, “Lexicon,” May 2019. Accessed February 24, 2020. <http://markets.ft.com/research/Lexicon/>.



## Ready for Next Step If You Have...

- Concluded necessary analysis and documented the methodologies used
- Synthesized results from different analytical processes in order to facilitate identification of key themes/findings and remaining knowledge gaps
- Considered strategies for communicating technical results with disparate stakeholder groups
- Validated analysis results through reviews with key partners and subject matter experts, as appropriate
- Addressed identified research questions to fullest extent possible

# STEP 5 DOCUMENT AND DELIVER RESULTS



With analysis activities complete, the next step is to aggregate important findings from the analysis, document the results, and identify ways to present the information in a manner that most effectively addresses the original purpose and goals intended outcomes of the assessment. Key steps in this process include identifying the most compelling results and framing them as digestible findings for stakeholders; developing potential courses of action that address resilience gaps identified through the assessment process; presenting the results in formats that can effectively communicate information while also protecting information security and sensitive data; and sharing the results with key partners to maintain buy-in and frame a strategy for action based on final outputs.



### Addressing Non-Technical Audiences

In the dozens of past assessments conducted through the RRAP, the intended audience has most often been dominated by personnel who are not technical experts in specific infrastructure systems. Rather, these assessments have usually been geared towards officials that have broad-based disaster planning, response and recovery responsibilities that cut across industries and infrastructure types. Typically, RRAP projects have sought to educate such “non-expert” audiences on important points of convergence and dependence among individual infrastructure systems in order to improve integrated planning and readiness.

volume of interest only to technical experts. Rather, the results should be shared with a potentially wide audience of government, private sector, and non-profit entities with different professional backgrounds and areas of focus who have a recognizable stake in the issues the assessment explored. Regional resilience assessments will likely involve stakeholders from different disciplines (e.g., urban planning, system operations, engineering, emergency management, and security) with different technical expertise, roles, and responsibilities. Thus, summarizing the bottom line results of the assessment and the associated recommendations for next steps has to resonate with a diverse set of partners.

A useful way to approach capturing the bottom line is to synthesize results into key findings and link potential courses of action to those findings. Key findings should succinctly communicate important observations from the analysis and explicitly outline how they relate to the resilience of the regional infrastructure being studied. The issues identified in key findings may tie back to technical specifications associated with the infrastructure, potential failure points identified through the analysis, stovepipes between key partners that create operational and governance challenges, or seams in steady-state and emergency planning frameworks, among other issues. Note that findings need not be exclusively focused on gaps or problems; findings that establish that certain effective practices are in place, or that

## Documenting Results

The final results for the type of collaborative regional infrastructure resilience assessment described in this document should not reflect a strictly academic exercise that explored theoretical challenges and culminated in a dense

the consequences of a possible hazard are less than expected are valuable in their own right. Good practices deserve to be documented and shared, and a truer appreciation for risks (whether high or low) is always valuable when considering how time and resources will be directed. Aggregating results into a manageable portfolio of key findings (e.g., RRAP project reports often have four to six key findings) makes the results easier to digest, simpler to communicate, and more compelling to adjudicate.



### Crafting Effective Key Findings

While the substance and argument behind certain key findings may seem clear, relevant messages must be constructed and communicated in a way that adheres to the understanding and agreements that underpin the assessment. For example, it can be tempting to ground a key finding in a very specific vulnerability or gap that ties back to a particular organization. But doing so may violate the terms on which that organization voluntarily agreed to participate in the assessment. Similarly, a key finding may highlight a shortcoming of a specific government agency that cannot rectify the issue without legislative changes. In these and other cases, key findings must be communicated in ways that honor the voluntary nature of the assessment and avoid inappropriate scrutiny of specific participants.

### Developing Courses of Action

Identifying resilience issues is a necessary step in any assessment; however, to be an effective tool for motivating change, a collaborative regional resilience assessment should go further to identify potential courses of action to improve resilience. This type of collaborative assessment should take advantage of the experience and perspective of

its stakeholders to not only enable identification of issues but also to envision their solutions. Potential courses of action should be developed and socialized with assessment partners, especially those who may have a role in carrying them out. This helps ensure that they identify appropriate organizations as their agents, are logical and feasible proposals, and identify known resources that can assist in their execution.

Well-constructed courses of action should do the following:

- Clearly identify organizations that should lead or otherwise have a role in their execution;
- Be logical solutions that are relevant to the issue identified in the key finding;
- Be realistically feasible within known constraints; and
- Identify available resources that can assist in their execution.

Given the range of participants in the assessment process, it can also be helpful to anchor potential courses of action in other organizational frameworks that may resonate with these communities. For example, the five mission areas outlined in the *National Preparedness Goal* may be a useful way to organize recommendations; grouping potential actions into these categories can help focus on relevant stakeholders (see table 17). For example, prevention efforts would likely align more closely to participants with security responsibilities, while mitigation activities would tend toward urban planners and engineers. Alternatively, elements of capability (i.e., planning, organization, equipment, training, exercises) provide another way to structure thought-processes when considering what might be appropriate actions to address an observed resilience shortfall (see table 17). Was the issue predominantly a result of inadequate planning, organization, lack of equipment, insufficient training, or lack of familiarity with all of the above that could be resolved through exercises? These categories are also used in certain homeland security grant programs to identify allowable costs and should translate well into such investment justification processes.



## Gaining Buy-in for Courses of Action

While the assessment must remain objective at all times, in many cases reviewing proposed courses of action with relevant participants and stakeholders is prudent prior to finalizing an assessment report. Every course of action has a cost of type, timeframe, potential regulatory nexus, and other potentially unforeseen barriers. In addition, a given course of action may have been considered already and rejected (or even unsuccessfully pursued) for important and valid reasons. Proposed courses of action cannot just be “good ideas,” but must be based in reality and open to implementation by participating organizations.

**TABLE 17**  
**Options for Organizing Assessment Recommendations**

Preparedness Mission Areas	Elements of Capability
Prevention	Planning
Protection	Organization
Mitigation	Equipment
Response	Training
Recovery	Exercises

## Presenting the Information

The assessment’s key findings and associated courses of action, as well as the body of research and analysis, need to be presented to stakeholders in a compelling and useful format (or multiple formats) that meets their intended uses. These can take various forms. Example outputs from a regional resilience assessment include a range of products such as these:

- Narrative reports that document analysis, key findings, and recommendations. Narrative reports can include executive summaries that document only the highlights of the effort; more detailed summary reports for a broader audience with moderate technical background; and longer technical reports for subject matter experts who are interested in exploring more detailed methodological topics.
- Checklists that document vulnerabilities at the asset- or system-levels and options for consideration to mitigate those vulnerabilities. These resources can serve as action-oriented roadmaps for stakeholders to consider as they explore potential resilience enhancement options.
- Briefings and presentations for delivery at interagency meetings, workshops, or industry/academic conferences. These presentations allow stakeholders to tell the broader story of the regional resilience assessment in a more concise and digestible format.
- Infographics that represent data and findings from the assessment in visually compelling formats that make it easier for users to understand and process important results.

- Static and interactive mapping products that leverage geospatial data and analysis collected during the assessment to illustrate relevant findings and recommendations related to regional infrastructure systems. Static maps can be incorporated into other products, while interactive maps are more dynamic resources that stakeholders can apply to address questions as they arise.
- Decision support tools that help stakeholders test potential courses of action in order to make informed decisions. These tools can include straightforward checklists and decision trees within a simple user interface or more advanced software options that integrate models and visualization elements.

- Compiled datasets, such as geospatial information, modeling outputs, and asset inventories that were collected, curated, or created during the process of performing the resilience analysis can also provide value to the stakeholders for further planning and analysis. These resources can be used as stand-alone capabilities or incorporated into existing information sharing and analysis portals used by relevant stakeholders.

Analytical approaches taken in different assessment types can generate a range of potential outputs that vary across assessments, as shown in table 18.

**TABLE 18**  
**Example Outputs for Regional Infrastructure Resilience Assessments**

Types of Resilience Assessments	Example Outputs
Assessments focusing on characterizing infrastructure systems and their dependencies and interdependencies	<ul style="list-style-type: none"> <li>■ Detailed infrastructure maps, geospatial data layers, and interactive presentations</li> <li>■ Diagrams of operations and technologies</li> <li>■ Depictions of organizational relationships</li> <li>■ Identification of important facilities and system functions</li> <li>■ Maps and diagrams that describe important regional infrastructure systems and their dependencies/interdependencies</li> <li>■ Detailed examinations of specific dependencies/interdependencies across one or more systems</li> <li>■ Associated analysis of the strength of dependencies/interdependencies and operational alternatives</li> </ul>
Assessments focusing on understanding the consequences from specific threats and hazards on infrastructure systems	<ul style="list-style-type: none"> <li>■ Modeling and analysis of infrastructure and cascading impacts, with associated maps and diagrams</li> <li>■ Examination of potential infrastructure alternatives or mitigation measures for infrastructure systems</li> <li>■ Review of and updates to hazard-specific plans and strategies</li> <li>■ Inputs to community resilience planning processes</li> </ul>

## Sharing Results

After identifying and documenting meaningful results from a regional assessment, an important next step is to share draft and final results with stakeholders. For key stakeholders who participated in data collection activities or are primary audiences for the results of the assessment, sharing preliminary drafts of outputs is a suggested practice that can help maintain their buy-in for the effort, offer opportunities for validation and refinement of findings, and generate ideas for ways to close identified resilience gaps. This type of information sharing on draft materials can occur through a range of mechanisms, including in-person briefings, where preliminary results are shared through presentations and verbal discussion, and remote desk reviews of draft documents, where stakeholders have the chance to provide detailed comments and edits. In some cases, a mix of these approaches may be appropriate, depending on the number of stakeholders, logistical considerations, practical time constraints, and the nature of anticipated feedback. In addition, spending relatively more time in the review and validation phase with a handful of critical stakeholders may be prudent in order to ensure they have visibility into the results at a level of detail that is commensurate with their involvement in the assessment.

As the results are finalized, assessment teams can prepare a dissemination strategy to guide decisions about what information they want to share with whom and when. For example, written documentation could be shared with participants and, if information security considerations allow, also disseminated more broadly to communities outside the established set of stakeholders (e.g., university researchers, community organizations, federal partners with a regional presence). Depending on the assessment, some materials may be germane to a broad audience (e.g., overall summary report or executive summary), while other outputs may be targeted to a specific audience (e.g., data layers for GIS team, technical reports for specific agencies, site-specific findings for a specific infrastructure owner). Outbriefs and workshops offer additional avenues for sharing results with interested parties, centered on outlining outcomes from the assessment, discussing possible next steps, and providing in-depth reviews on particular technical analyses.

## Guiding Principles for Product Development

The topics, scopes, data, analyses, and associated outputs for regional resilience assessments can vary widely across communities and regions. However, several basic guiding principles for product development merit consideration regardless of the assessment's complexity.

- **Refer back to original assessment objectives and desired outcomes:** build products that convey research and analytic results in a way that achieves desired stakeholder outcomes. Results from discussions with stakeholders during the scoping phase can be particularly helpful in this regard, providing clearer criteria driven by end-users on what they expect to come from the assessment process and how they hope to use those results.
- **Write clearly and concisely:** particularly when trying to appeal to a broad audience with a range of technical backgrounds, writing clearly and concisely is important. If narrative reports are laden with jargon or dedicate long sections to methodological explanations and caveats, the audience may not draw the desired conclusions or find the document useful.
- **Follow sound research practices:** at their core, regional resilience assessments are research assessments that involve a mix of methods and technical approaches. In documenting results, the basic guidelines for analytical writing apply. These include, but are not limited to, supporting assertions with evidence; avoiding inclusion of personal opinions; documenting and citing sources appropriately; subdividing large concepts into more manageable segments; and communicating relevant research questions and structuring the analysis to support it.
- **Use graphics:** combining narrative with maps, process flows, system diagrams, data tables, charts, and graphs is a more effective mechanism for communicating results than text alone. These visuals also provide important foundational elements for briefings and infographics.

- **Share drafts with stakeholders for review:** formal and informal reviews of draft outputs provide stakeholders with opportunities to clarify the inputs they provided, refine modeling assumptions, confirm accuracy of content, and solicit buy-in before the materials are released more broadly. The review process should elicit specific and actionable feedback for the authors and improve the defensibility of the product.
- **Plan a dissemination strategy:** regional resilience assessments can involve literally dozens of stakeholders throughout their lifecycles. Participants can include core stakeholders from government and private sector who advocated for and drove the assessment initially; additional organizations that contributed to the data collection and analysis efforts; broader community organizations with an indirect interest in the results; academic and research organizations with a substantive interest in the analysis; and even the general public. Core stakeholders should agree on a strategy for what outputs will be released to which constituent groups

and how. An additional factor to consider is communicating where pertinent information will be stored and in what format in order to facilitate knowledge management upon conclusion of the assessment.

- **Consider information security:** proper protection and handling of all materials developed during the assessment process are paramount. Historically, some resilience assessment products have been considered sensitive. For instance, some final outputs from DHS-sponsored RRAP projects have been designated as FOUO or PCII. However, stakeholders have been increasingly interested in developing and sharing completely open-source products (e.g., brochures, briefings) without any sensitive information or its associated dissemination controls. Because the nature of the infrastructure resilience mission demands sharing—and over-restricting information impedes the ability of partners to work across sectors within their region to build resilience—they often seek wider dissemination of products to a broader audience.



### Ready for Next Step If You Have...

- Crafted key findings that summarize results of resilience assessment for diverse stakeholder audiences
- Identified relevant courses of action to address resilience gaps
- Identified and developed different products through which to present assessment results to relevant audiences
- Engaged stakeholders on strategies for acting collaboratively implementing identified resilience enhancement efforts
- Confirmed with stakeholders the path forward for information sharing and information protection

## STEP 6 PROMOTE ACTION



While the assessment’s data gathering, analysis, and various outputs are significant outcomes in and of themselves, they do not constitute the conclusion of the regional effort. The outputs from the resilience assessment are actually intended to be part of a longer-term risk management process that leads to meaningful, measurable progress in improving regional resilience by stimulating continued cooperative action. Implementing discrete measures to improve infrastructure resilience can strengthen and sustain partnerships that were developed and expanded during the course of the regional assessment.

Potential courses of action that emerge from an assessment could include steps to address resilience gaps identified during the analysis and to sustain existing capabilities that are important to regional resilience. The goal of the assessment process is not simply to highlight resilience gaps and areas of improvement for stakeholder consideration. Effective regional resilience assessments should go beyond these high-level steps and include specific options for stakeholder consideration to mitigate those issues. In other words, the assessment should identify what challenges exist, what can be done to address them, and who can implement these suggestions.

However, taking action to strengthen infrastructure resilience—whether through planning processes, capital investments, new personnel, information sharing, training, or exercises—is inherently complicated and will likely stretch beyond the responsibilities and authority of the team of analysts conducting the assessment. The assessment approach outlined in this document is intended to contribute objective analysis to decision makers in government and the private sector for review and consideration. Political realities, budget constraints, governance complexities, and the cross-sector stakeholder landscape are basic realities that regional partners must navigate as they look to address findings identified in assessment processes. These challenges are particularly notable given that assessments are often voluntary efforts, with

no enforceable requirements to address issues that they identify and no regulatory mandate to implement recommendations. Obtaining buy-in from key partners during the initial problem identification and scoping phases of the resilience assessment, and maintaining partner engagement throughout the assessment, are thus critical to increasing the likelihood of partner action to act upon findings and recommended actions. The results from resilience analysis can spur action and deliver value to stakeholders, but it is important to manage expectations about how quickly and comprehensively regions can engage disparate partners collaboratively to tackle significant issues identified in assessments, given practical political and economic realities facing communities and businesses nationwide.

### Managing Risk Through Resilience Enhancements

The overall risk environment facing critical infrastructure partners is such that no single entity can manage risks entirely on its own. Given this shared risk, partners benefit from access to knowledge and capabilities that would otherwise be unavailable to them.<sup>50</sup> Ultimately, the work that follows and is informed by the assessment process is about managing risk to regional infrastructure: implementing resilience solutions and measuring their effectiveness.

<sup>50</sup> CISA, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

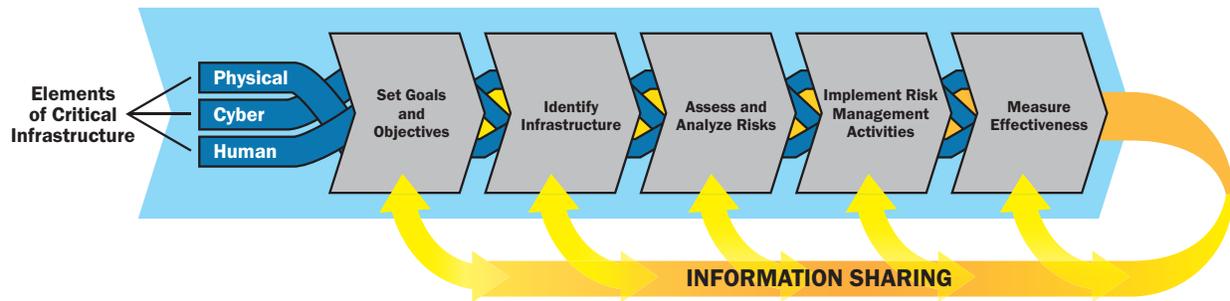


FIGURE 11.—Critical Infrastructure Risk Management Framework.

Risk management is a process that examines and weighs policies, plans, and actions for reducing the impact of a hazard or hazards on people, property, and the environment. Ideally, risk is managed in the most effective and equitable way subject to available resources and technical capabilities. Under the best circumstances, risk management includes risk-reduction strategies that draw upon scientific, engineering, social, economic, and political expertise. An important aspect of risk management is providing realistic expectations as to what can be accomplished using specific strategies and the relative costs and benefits of undertaking proposed measures. Managing expectations is also important because disaster risks cannot be eliminated completely even with the most appropriate and successful risk management strategies. In addition, some tools or actions that can reduce short-term risk may increase long-term risk, requiring careful evaluation of the risk management strategies employed. Although some residual risk will always require attention, risk management can help build capacity to become more resilient to disasters, particularly when everyone in a community is engaged in managing risk.<sup>51</sup>

Figure 11 shows the critical infrastructure risk management framework outlined in the NIPP, which outlines an iterative process for reevaluating risks in light of new information (e.g., findings from a regional infrastructure resilience assessment) and incorporating it back into the overall risk management process. This framework is flexible enough for use in all sectors, across different geographic regions, and by various partners. It supports a decision-making process that critical

infrastructure partners collaboratively undertake to inform the selection of specific actions that address identified risks.<sup>52</sup>

### Example Actions to Enhance Regional Infrastructure Resilience

While assessment outputs convey the results of the analysis and offer suggested actions to enhance resilience, the work that follows an assessment centers on stakeholders using results to take action to address identified resilience gaps. Some activities may be identified early in the scoping process, while others may emerge as new issues are revealed through data collection and analysis. The sections below describe broad categories of actions that can result from regional infrastructure assessment efforts.

#### Planning

A typical activity arising out of regional infrastructure resilience assessments is the need to develop or update plans, including strategic, operational, and tactical plans. Specific examples include regional emergency operations plans; business continuity plans; state and local mitigation plans; hazard-specific annexes (e.g., long-term power outage); and state and local hazard mitigation plans. Other planning processes include joint working groups involving government and industry partners around shared issues of concern (e.g., potential disruptions at a port). Those engagements may focus on sharing assessment results to enhance participant

<sup>51</sup> National Research Council. *Disaster Resilience: A National Imperative* (Washington, DC: The National Academies Press, 2012).

<sup>52</sup> CISA, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. 2013. Accessed February 13, 2020. [www.cisa.gov/national-infrastructure-protection-plan](http://www.cisa.gov/national-infrastructure-protection-plan).

understanding of potential issues (e.g., supply chains and logistics) and foster greater coordination between industry and government agencies on potential mitigation measures.



## National Mitigation Investment Strategy

In August 2019, FEMA released the National Mitigation Investment Strategy which includes goals for enhancing mitigation nationally, recommendations on how to approach them, and examples from communities nationwide.

**Goal 1:** Show how mitigation investments reduce risk

- Recommendations: make mitigation investment relevant; increase mitigation investment by building the capacity of communities to reduce their risks; use common measures to aid decision-making for mitigation investment

**Goal 2:** Coordinate mitigation investments to reduce risk

- Recommendations: Make risk information more available and easier to use; align program requirements and incentives; make funding for mitigation investment easier to access

**Goal 3:** Make mitigation investment standard practice

- Recommendations: Encourage communities to adopt and enforce up-to-date building codes; strengthen critical infrastructure and lifelines; use and expand financial products and approaches to reduce and transfer risk

The strategy is available via FEMA here: [www.fema.gov/emergency-managers/national-preparedness/frameworks/mitigation/mitflg](http://www.fema.gov/emergency-managers/national-preparedness/frameworks/mitigation/mitflg).

## Capital Investments and Grant Submissions

Another typical implementation activity is providing justification for capital investments and grant submissions. Critical infrastructure owners and operators in a region increasingly recognize the need for investment in innovative infrastructure upgrades, both in the short term and over longer timeframes, to make infrastructures more resilient and protected against risks the region has not yet faced. Therefore, facility owners and operators, regional organizations, and government agencies can use the resilience analysis findings to guide strategic investments in equipment, planning, training, and resources to enhance the resilience and protection of facilities, surrounding communities, and entire regions. For example, a potential option for increasing the resilience posture of a system includes exploring the creation of a public-private partnerships to increase funding.

Incorporating resilience is not a new concept for investors. For example, when planning new investments, it is standard practice for investors to perform cost-benefit analyses. These analyses and other tools enable investors to make well-informed decisions that lead to smart, profitable investments. Critical infrastructure investors also have an incentive to be forward-looking, since the lifespan of many types of infrastructure can be 50 to 100 years. Prior to funding a project, investors and project managers will generally try to identify the impacts of demographic and population trends so they can determine whether the critical infrastructure they develop will retain its usefulness over the infrastructure’s lifetime.<sup>53</sup>

However, justifying large capital investments in resilient infrastructure is often difficult without public support and the ability to recoup costs. Recent experience with losses from catastrophic events like Hurricane Sandy provides tangible evidence of the economic and public health consequences of weak infrastructures. The unprecedented flooding and damage that occurred during Hurricane Sandy caught many operators and public officials off guard, creating a strong business case in the public and private sectors for billions of dollars of investment in infrastructure hardening and technology upgrades.

<sup>53</sup> CISA, *NIPP Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects*. Undated. Accessed February 13, 2020. [www.cisa.gov/publication/nipp-2013-resilience-ci-projects](http://www.cisa.gov/publication/nipp-2013-resilience-ci-projects).

In addition, prior investment in fiber cable and undergrounding for resilience paid off for communications companies. On the same streets in lower Manhattan, tons of copper cable were corroded by saltwater, while fiber lit back up once switches came back online; even above ground, fiber did not break as often as copper. Conversely, in areas where the business case for these investments does exist, rate recovery for resilience investments can be a political challenge, even after large storms.<sup>54</sup>



## Building Resilient Infrastructure and Communities (BRIC) Grant Program

Signed into law in October 2018, the Disaster Recovery Reform Act included significant reforms to federal disaster programs. Included in the legislation were changes to pre-disaster mitigation funding available to communities across the country. Through this effort, FEMA is creating a new grant program called Building Resilient Infrastructure and Communities (BRIC), which will help manage risk nationally by funding public infrastructure projects that increase a community's resilience before a disaster affects an area. This program will be funded annually through the Disaster Relief Fund as a six percent set-aside from estimated disaster grant expenditures. Results from regional infrastructure resilience assessments would be useful inputs for communities to use in shaping potential projects under this program. Updates on FEMA's BRIC program are available at: <https://www.fema.gov/drra-bric>.

## Training

Assessment findings may point to training gaps for government and private sector partners. These training needs can include general training on core issues (e.g., incident management) or organization-specific training tied to internal policies and procedures (e.g., ensuring staff have awareness of business continuity or emergency operations plan). A variety of applicable training programs and courses are offered by different federal, state, and local agencies, as well as private partners and industry associations. For example, FEMA provides dozens of mobile, in-residence, and independent study courses through its Emergency Management Institute, Center for Domestic Preparedness, and National Training and Education Division. FEMA also sponsors the Rural Domestic Preparedness Consortium, which has developed training in support of rural homeland security requirements. CISA offers additional training on general infrastructure security issues as well as sector-specific topics (e.g., chemical, commercial facilities, dams, emergency services).

## Exercises

Identifying and assessing risks and associated impacts helps organizations identify priorities, objectives, and core capabilities to be evaluated through exercises. Exercises are an excellent means of further exploring newly identified risks, resolving coordination and planning gaps, and devising approaches to other infrastructure issues identified during the course of a regional resilience assessment. Exercises can enable stakeholders to test and validate plans and capabilities, and identify gaps and areas for improvement. A well-designed exercise provides a low-risk environment to test capabilities, familiarize personnel with roles and responsibilities, and foster meaningful interaction and communication across organizations.<sup>55</sup> Exercises are cost-effective and useful tools that help the participants practice and refine specific capabilities. Exercise objectives are distinct critical elements necessary to achieve specific mission area(s) and can be described in terms of expected outcomes for the exercise.

<sup>54</sup> NIAC, *Strengthening Regional Resilience: Final Report and Recommendations*. November 2013. Accessed February 13, 2020. [www.cisa.gov/niac-reports-and-recommendations](http://www.cisa.gov/niac-reports-and-recommendations).

<sup>55</sup> FEMA, *Homeland Security Exercise Evaluation Program*, January 2020, Accessed August 24, 2020. [www.fema.gov/emergency-managers/national-preparedness/exercises/hseep](http://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep).

Example exercise objectives related to infrastructure resilience can include the following:

- Reviewing existing preparedness, response, and recovery plans, policies, and procedures of both public and private sector participants related to the disaster being exercised
- Examining and assessing the existing relationships between federal, state, and local government entities and the private sector infrastructure located in the area under study
- Assessing the cascading effects at a local, regional, and national level of the disaster, with a focus on potential disruptions to infrastructure systems

Discussion-based exercises include seminars, workshops, tabletop exercises, and games. These types of exercises can be used to familiarize players with, or develop new, plans, policies, agreements, and procedures. Discussion-based exercises focus on strategic, policy-oriented issues. Facilitators and/or presenters usually lead the discussion, keeping participants on track towards meeting exercise objectives. Operations-based exercises include drills, functional exercises, and full-scale exercises. These exercises can be used to validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps. Operations-based exercises include a real-time response to an exercise scenario, such as initiating communications or mobilizing personnel and resources.<sup>56</sup>

### Tracking Progress

An enduring part of the regional infrastructure resilience assessment process is to document outcomes and track progress in enhancing regional resilience. Each action taken should have a clear measure (or set of measures) associated with it that allows stakeholders to better understand and communicate the impact of activities pursued. Moreover, the sponsoring organizations should be able to characterize why the effort was important and how it made a difference to the region. Example considerations in gauging the value of the overall assessment include the following:

- Demonstration of enhanced resilience during real-world events
- Cost/benefit analyses and return on investment analyses of specific capital investments
- Plans developed or updated based on assessment findings
- Training conducted to address identified knowledge gaps
- Specific issues identified in exercises that are addressed through continuous improvement planning

Regional resilience assessments can lead to substantial achievements and progress for participating organizations. The analysis conducted can close significant knowledge gaps, helping participants understand particular issues, assets, or scenarios that are of greatest importance to sustaining operations. The process can lead to the creation of new decision-support tools and visualizations that inform planning and investment decisions for years to come. Yet even with tangible successes that arise from assessments, fundamental challenges may still exist that can impede progress, including the following:

- Stakeholder fatigue
- Resource constraints
- Competing priorities
- Technology limitations
- Legal and regulatory delays
- Leadership changes
- Complicated governance

Anticipating these challenges and trying to manage against them requires continuous attention in order to lessen the likelihood that they derail implementation of recommended activities that improve the resilience of infrastructure regionally.

<sup>56</sup> FEMA, *Homeland Security Exercise Evaluation Program*, January 2020, Accessed August 24, 2020. [www.fema.gov/emergency-managers/national-preparedness/exercises/hseep](http://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep).



## Achieved Success If You Have...

- Established a process for documenting outcomes from the assessment and tracking progress in enhancing regional resilience
- Developed and applied an engagement strategy for sharing updates with stakeholders on progress and notable accomplishments arising from the assessment
- Used planning, training, exercises, investments, and other mechanisms to enhance the resilience of regional infrastructure



# TYING IT ALL TOGETHER

The preceding sections outlined a stakeholder-driven, partnership-focused, six-step process for assessing critical infrastructure resilience on a regional scale. Although each section features a series of examples and tips for readers to consider, stepping back and reviewing how each stage unfolded from start-to-finish in the context of a single project may be a useful way to illustrate the wide range of partners, issues, techniques, and products that can be associated with assessment efforts. The pages that follow outline four different regional resiliency assessments, highlighting partner engagement approaches and activities to move from problem identification through analysis to final products and action.



- 1. Identify Problem:** while the idea for a resilience assessment can originate from a variety of sources, this important first step begins with identifying a problem that regional partners need to address and developing a concept that they can execute together.
- 2. Design Assessment:** this step involves defining the key research questions that regional assessment efforts will attempt to address, establishing the geographic extent of the effort, identifying infrastructure systems to be considered in the assessment, and articulating the specific steps that stakeholders will take to address key research questions.
- 3. Collect Data:** activities can include open-source research, multi-agency collaboration, subject matter expert interviews, facilitated discussions, site assessments, and other steps that help stakeholders capture information needed to address the assessment’s key research questions.
- 4. Analyze:** this step involves the application of an analytical approach that incorporates one or more analytical techniques (e.g., geospatial analysis, modeling and simulation) to evaluate the infrastructure systems of interest.
- 5. Document and Deliver Results:** this step centers on documenting specific issues, challenges, and opportunities discovered through the assessment and defining potential courses of action that can begin to address identified resilience gaps.
- 6. Promote Action:** the final step involves laying the groundwork for action on analytical findings and taking tangible steps to enhance resilience through capital investments, planning efforts, training, and exercises.

# REGIONAL ASSESSMENT OF NATIONALLY-CRITICAL DATA CENTERS

The cluster of data centers in the greater Ashburn area in Loudoun County, Virginia serves as the primary global Internet traffic hub on the East Coast owing to the presence of a major Internet exchange point. This project focused on assessing the resilience of this Internet backbone infrastructure.

Step	Ashburn, Virginia Data Center Project Activities
<p><b>Engaging Partners</b></p>	<p>A wide range of public and private stakeholders participated in the scoping, data-gathering, and analysis activities of this project. These engagements included opportunities for stakeholders to engage in forums that allowed them to focus on resilience of Internet infrastructure.</p> <p>Under the auspices of this project, nearly two dozen meetings occurred with private and/or public sector stakeholders. Project team members attended and briefed attendees at regular meetings of the North American Network Operators Group, which is the professional association for Internet engineering, architecture, and operations. The project team conducted a facilitated discussion that included more than 70 participants from across the region, including data center owners and operators and regional emergency managers and first responders.</p> <p>Engagement also took place through the following:</p> <ul style="list-style-type: none"> <li>■ Scoping meetings</li> <li>■ General information sharing conference calls</li> <li>■ Regular status meetings and in-progress reviews</li> <li>■ Discussions to inform analysis assumptions and refine analytic approaches</li> <li>■ Meetings to review and validate findings</li> <li>■ Reviews of draft outputs</li> <li>■ Outbriefs with team members, key stakeholders, and leadership to share results</li> </ul>
<p><b>Problem Identification</b></p>	<p>With the unique concentration of both fiber and power, on average, 50-70 percent of all Internet traffic flows through the greater Ashburn-area data centers. Greater Ashburn-area data centers provide primary and secondary continuity and backup for the IT infrastructure of federal, state, and local governments. The protection of network and data infrastructure assets in the greater Ashburn-area is critical to the continuity of operations of governmental agencies and private companies that, in turn, supply day-to-day services to utilities and the public.</p>

Step	Ashburn, Virginia Data Center Project Activities
<b>Assessment Design</b>	The project sought to identify vulnerabilities of Internet assets that could affect the community’s ability to recover from the impacts of a variety of natural and human-caused hazards. The infrastructure that was examined included individual fiber routes and installations; data centers; communications providers; and the power, water, and emergency services sectors that support Internet infrastructure. The project focused on improving communication and information sharing between stakeholders, including data center representatives and first responders in the community.
<b>Data Collection</b>	Data collection approaches included literature review, open-source research, access to controlled data sets, facilitated discussions, and one-on-one interviews. The data center market is highly competitive, and secrecy about operational details is a standard procedure. Thus, information security was an important factor in gaining buy-in from stakeholders to participate. Some of this information is designated as FOUO, a designation for documents with unclassified information of a sensitive nature, not otherwise categorized by statute or regulation.
<b>Resilience Analysis</b>	Resilience analysis techniques focused on understanding the resilience of Internet infrastructure. Data collected through facilitated discussions and interviews were the key inputs to the analysis and resulting key findings. The project activities allowed participants to collaborate openly and demonstrate the community’s commitment to a common goal of network and data resilience. The analysis used electric power contingency modeling to identify areas that would lose power due to disruptions to key substations serving the Ashburn region.
<b>Documenting and Delivering Results</b>	The project team prepared a report with both narrative and maps to summarize the key findings and potential courses of action identified in the project. The report was prepared for the Virginia Office of Public Safety and Homeland Security for distribution to partner organizations and local business representatives who participated in the project and have a need to know the information. As a related activity, the project team also organized a seminar on electromagnetic pulse issues for data center providers.
<b>Promoting Action</b>	This project communicated key findings and provided resilience enhancement options that can support local, state, federal, and private sector organizations’ efforts to close gaps in Internet infrastructure and operational resilience.

# REGIONAL ASSESSMENT OF ELECTRICITY, TRANSPORTATION, AND COMMUNICATION INFRASTRUCTURE

New York City continues to address lessons learned from Hurricane Sandy’s impacts on its infrastructure in 2012. As part of these efforts, the city is planning to protect critical assets and systems from extreme weather events through resilient design. To assist New York City, this project provided a cross-sector review of the regional energy, transportation, and communications infrastructure at risk from future extreme weather events.

Step	New York City Electricity, Transportation, and Communications Project Activities
<b>Engaging Partners</b>	<p>The New York City Mayor’s Office of Recovery and Resiliency (ORR) was the primary partner for this project. Extensive engagement with ORR, the New York City Panel on Climate Change, other city and state government departments, and infrastructure owners and operators took place throughout the project. Mechanisms used to engage these partners included the following:</p> <ul style="list-style-type: none"> <li>■ Discussions with existing working groups, centered on infrastructure resilience challenges</li> <li>■ Scoping meetings</li> <li>■ Regular status meetings</li> <li>■ Engagements about data sharing and protection</li> <li>■ Discussions to inform analysis assumptions and refine analytic approaches</li> <li>■ Meetings to review and validate findings</li> <li>■ Outbriefs with team members, key stakeholders, and leadership to share results</li> <li>■ Follow-ups to scope next steps and implementation priorities</li> <li>■ Supplemental engagements on understanding and using results</li> </ul>

Step	New York City Electricity, Transportation, and Communications Project Activities
<b>Problem Identification</b>	The impacts to critical infrastructure from Hurricane Sandy storm surge and projections of future extreme weather due to climate change.
<b>Assessment Design</b>	This project identifies infrastructure vulnerabilities to future extreme weather events and high-consequence failure points for priority consideration in the city’s planning programs and specific resilient design projects to protect the city’s most vital infrastructure.
<b>Data Collection</b>	Data collection approaches included literature review, open-source research, accessing controlled data sets, and plan reviews. Project stakeholders provided downscaled climate data and infrastructure data at the asset level which was used to assess natural hazard vulnerability and to evaluate dependency risk. Proprietary system-level electric power data was purchased for modeling purposes.
<b>Resilience Analysis</b>	A key analysis approach in this project involved extensive modeling of projected mid-century electric power grid operations stressed by a long-duration heat wave and geospatial analysis of critical infrastructure resource flows. Using these inputs, the project team identified vulnerabilities (including dependencies and interdependences) that amplify system risk and high-consequence failure points that could result from future extreme weather events.
<b>Documenting and Delivering Results</b>	The team provided a resilience assessment report, electric-power modeling technical report, dependency analysis technical report, and corresponding geospatial analysis map book and data to New York City.
<b>Promoting Action</b>	New York City is using output from the project to identify priority areas and corridors for future resilience investments, which are documented through OneNYC, the planning process to build a stronger, more resilient New York City.

# REGIONAL ASSESSMENT OF SURFACE TRANSPORTATION SYSTEMS

This project assessed the resilience of Washington State’s surface transportation systems to a Cascadia Subduction Zone (CSZ) earthquake, and the ability of those systems to support post-disaster response and recovery activities. A key outcome of this project was the identification of priority highway routes into western Washington which will be better able to support the movement of resources into the affected area. These results are based on extensive network- and system-level assessments of highway transportation infrastructure, using seismic screening tools developed as part of the project.

Step	Washington Transportation Systems Project Activities
<p><b>Engaging Partners</b></p>	<p>The project facilitated collaboration among regional stakeholders to assess the seismic resilience of the state’s surface transportation system. The project team engaged stakeholders from federal, state, county, and municipal governments, as well as from the private sector. The Washington State Military Department’s Emergency Management Division (EMD) was the regional sponsor for this project. In addition to EMD, four organizations participated as core stakeholders, offering input on the project’s scope, approach, methodologies, analytical outcomes, and findings. This core stakeholder group included the following organizations:</p> <ul style="list-style-type: none"> <li>■ Washington State Department of Transportation</li> <li>■ FEMA, Region X</li> <li>■ USCG, District 13</li> <li>■ U.S. DOT, Region X</li> </ul> <p>Engagement took place through the following:</p> <ul style="list-style-type: none"> <li>■ Discussions with existing working groups</li> <li>■ Scoping meetings</li> <li>■ General information-sharing conference calls</li> <li>■ Regular status meetings and in-progress reviews</li> <li>■ Discussions to inform analysis assumptions and refine analytic approaches</li> <li>■ Meetings to review and validate findings</li> <li>■ Reviews of draft outputs</li> <li>■ Outbriefs with team members, key stakeholders, and leadership to share results</li> <li>■ Supplemental engagements on understanding and using results</li> </ul>

Step	Washington Transportation Systems Project Activities
<b>Problem Identification</b>	The resilience of Washington State’s surface transportation systems to a CSZ earthquake, and the ability of those systems to support post-disaster response and recovery activities.
<b>Assessment Design</b>	The project team sought to provide information that prioritizes state highway routes to act as transportation links between staging areas for CSZ response and recovery efforts.
<b>Data Collection</b>	Data collection approaches included literature review, open-source research, accessing controlled data sets, and plan reviews. Specific data collected included detailed bridge structural information, highway network, emergency response plans, geologic data, and seismic data.
<b>Resilience Analysis</b>	Resilience analysis techniques focused on understanding the consequences of the CSZ event on the transportation system. The team used advanced modeling techniques and engineering assessments to inform the analysis and the resulting priority routes for emergency response.
<b>Documenting and Delivering Results</b>	The project delivered a narrative report with a series of findings and potential courses of action. The project team also created two screening tools to help identify seismic vulnerabilities in bridges and highways. These tools were shared with stakeholders for continued use following the conclusion of the project. The project also produced a range of geospatial analysis products.
<b>Promoting Action</b>	The Washington State Department of Transportation, one of the core stakeholders for the project, is integrating the outcomes of this project into funding priorities for its bridge seismic retrofit program, which will invest \$160 million over the next 8 years to retrofit infrastructure. Results will also inform earthquake response and restoration planning activities by FEMA, EMD, and local emergency management agencies.

# REGIONAL ASSESSMENT OF HEALTHCARE SUPPLY CHAINS

This project focused on building greater understanding of healthcare product supply chains serving a large metropolitan region, identifying risks of major supply-chain disruptions, and describing options for improving greater supply-chain resilience and preparedness across a diverse range of stakeholders.

Step	Healthcare Supply-Chain Project Activities
<p><b>Engaging Partners</b></p>	<p>Initial discussions with healthcare providers, product vendors and other stakeholders was required to fully define the categories of partners that needed to be involved. Over a few months of discussions and preliminary meetings, these categories were established and included individual healthcare providers, multi-provider groups such as trade associations and industry coalitions, product manufacturers, product distributors, transportation/logistics companies, other supply-chain service providers, and federal, state and municipal government agencies.</p> <p>After establishing these partner categories, outreach began. The project started with large hospitals in the metropolitan area who had already agreed to participation, and then systemically branched out to the various other partner categories. For the most part, the project team relied on referrals from the hospitals to their vendors and other supply-chain partners to make contact and seek project participation. As more organizations were contacted and agreed to participate, more referrals to other important potential participants were obtained.</p>
<p><b>Problem Identification</b></p>	<p>The concept for the project originated from concerns following several recent healthcare product supply-chain incidents, including impacts from an historic coastal storm, the H1N1 and Ebola outbreaks, and certain healthcare product shortages. Healthcare providers requested the project, recognizing that they needed to think more strategically about the supply chains that they rely upon, that the multitude of organizations involved in these supply chains needed to collaborate more, and that government must gain a better understanding of these supply chains if it is going to provide value during future incidents.</p>

**Step Healthcare Supply-Chain Project Activities**

<p><b>Assessment Design</b></p>	<p>Rather than addressing narrow, highly specific knowledge gaps, the project was designed to perform a broad-based examination of healthcare product supply chains serving this region. The healthcare providers that requested the project sought a “landscape view” of these supply chains, including how the supply chains are constructed, the major organizations involved, important operational and business considerations, the most concerning supply-chain risks, and opportunities to address gaps in current healthcare supply-chain disruption planning in the region.</p> <p>One important aspect that was not specific at the outset was the different categories of healthcare products for examination in the project. Therefore, initial interviews and consultations with industry partners led to identification of five major product categories: pharmaceuticals, medical-surgical supplies, blood products, medical gases, and medical linens.</p>
<p><b>Data Collection</b></p>	<p>The majority of data collection was conducted through one-on-one interviews, both in-person and via teleconference. In addition, some joint interviews and briefings involving multiple organizations took place. These data-collection activities centered on question sets that were designed to elicit a thorough understanding of each organization’s supply-chain operations. The questions focused on both normal and disrupted operations, seeking to determine the types of planning and capabilities in place to address supply-chain problems, and at what point outside assistance may arise. The question sets were customized for the type of organization (e.g., hospitals vs. suppliers vs. logistics providers). In addition to interviews, facility tours were conducted that provided a hands-on view of supply-chain operations (e.g., a hospital’s inventorying system, a supplier’s warehouse, a blood center’s processing facility).</p> <p>For government participants, questions focused on their level of understanding of healthcare supply chains, past events that required their involvement, their structure and decision-making for disaster response operations involving these supply chains, gaps in their planning and related topics.</p> <p>Few information security issues arose during data collection. The project was designed to stay at a fairly high level and avoid business proprietary and sensitive data. Most participants did not request special handling or data protection measures and were supportive of sharing viewpoints and experiences more broadly.</p>

**Step Healthcare Supply-Chain Project Activities**

**Resilience Analysis**

Given the project’s original design and the emphasis on providing a “landscape view” of these healthcare supply chains, the post-data collection effort focused on characterizing, visualizing, and documenting the large amounts of information provided by participants. The project did not focus on specific facilities or on specific quantitative measures. Rather, it was concerned with educating stakeholders on how these supply chains work, who is involved, and how can disruptions can occur. Therefore, the team used elements from various techniques to analyze and distill collected information. These included system diagramming (visualize how supply chains are constructed), consequence and vulnerability analysis (where along these supply chains can major disruptions occur and what could this entail), geospatial analysis (what is the geographic footprint for moving healthcare products into and around the region; where do critical distribution points exist in the region), and dependency analysis (what services/inputs are required along these supply chains to keep them operational).

**Documenting and Delivering Results**

This project led to the development of several products. A narrative report described the purpose and goals of the project, along with a variety of contextual information about normal healthcare supply-chain operations, and most importantly a series of key findings and future options for building greater resilience into the region’s healthcare supply-chain operations. In addition, a series of profiles for each of the five product categories was developed—these laid out in detail how each supply chain operates and where potential disruptions are possible. Maps of specific supply-chain facilities in the region were provided. Facilities included large supplier warehouses, oxygen and blood production sites, linen processing locations, and related infrastructure. An interactive diagram of all the healthcare product supply chains allowed users to visualize the different segments of these operations at different points in the process (i.e., from global to regional to local). Lastly, a resource was developed that described the types of supply-chain disruption scenarios that could confront the healthcare community. It described different types of challenges along with important planning aspects of each (e.g., cause, duration, complexity level, geographic scope, nature of required response).

All main participants were given an opportunity to review draft versions of relevant content to ensure accuracy and avoid the inclusion of any sensitive data. All of these products were packaged together and delivered electronically to all of the main project participants. Due to the agreed approach to avoid sensitive and proprietary information, information protection measures were not needed.

**Step Healthcare Supply-Chain Project Activities**

**Promoting Action**

The large and diverse set of participants in the project created important new partnerships for stakeholders in the region, including governmental organizations. These important connections between government and the healthcare industry have endured and helped to inform and propel follow-up activities and coordination related to healthcare supply-chain disruptions.

The project led to a large healthcare supply-chain workshop that focused on a scenario involving a protracted disruption to inbound healthcare products. The after-action report identified a variety of follow-up steps for the region to pursue. Individual hospitals in the region are using various resources that were produced as part of the project, such as the supply-chain profile resources that were developed for the various healthcare product types.

The project and its outcomes were featured in certain publications and presentations that have led to a much broader discussion among other regions on the need to examine and understand healthcare supply chains.

The success of the first project led to a follow-up effort that examined more detailed aspects of healthcare supply chains in the region, thereby solidifying a multiyear focus on this topic in this large metropolitan area.

The project has also enabled various Federal Government agencies to better understand each other’s roles, capabilities, and joint planning opportunities on topics related to healthcare supply chains and disaster preparedness.

## CONCLUSION

The methodology described in this document reflects countless lessons that CISA learned through the RRAP, but its application is intended to bolster capabilities of disparate organizations, communities, and regions to analyze, understand, and improve the resilience of critical infrastructure systems nationwide. Part 1 focused on defining the foundational concepts of resilience. Part 2 identified core elements of a general, scalable methodology for assessing the resilience of critical infrastructure, defining key processes and analytical techniques that can contribute to successful efforts. Together, the contents provide a roadmap that stakeholders—including federal and state, local, tribal, and territorial governments, and private sector owners and operators—can apply to their own needs.



## GLOSSARY OF KEY TERMS

**Consequence:** effect of an event, incident, or occurrence. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment

**Dependency:** a unidirectional relationship between two assets where the operations of one asset affect the operations of the other

**Hazard:** natural or man-made source or cause of harm or difficulty. A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed

**Interdependency:** a bidirectional relationship between two assets where the operations of both assets affect each other. An interdependency is effectively a combination of two dependencies

**Mitigation:** capabilities necessary to reduce loss of life and property by lessening the impact of disasters, including but not limited to community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred

**Prevention:** capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism, including but not limited to information sharing and warning; domestic counterterrorism; and preventing the acquisition or use of weapons of mass destruction

**Protection:** capabilities necessary to secure the homeland against acts of terrorism and human-caused or natural disasters, including but not limited to defense against threats from weapons of mass destruction; defense of agriculture and food; critical infrastructure protection; protection of key leadership and events; border security; maritime security; transportation security; immigration security; and cybersecurity

**Recovery:** capabilities necessary to assist communities affected by an incident to recover effectively, including but not limited to rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources

**Resilience:** 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

**Response:** capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred

**Risk:** potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

**Security:** reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or human-caused disasters

**Threat:** natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property

**Vulnerability:** qualitative or quantitative expression of the level to which an entity, asset, system, network, or geographic area is susceptible to harm when it experiences a hazard

