Proceedings of the 2018 Winter Simulation Conference
M. Rabe, A.A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, eds.

ASSESSING CRITICAL INFRASTRUCTURE DEPENDENCIES AND INTERDEPENDENCIES

Scott Breor

Department of Homeland Security
Office of Infrastructure Protection
245 Murray Lane
Washington D.C. 20598

ABSTRACT

Today's infrastructure is connected to many other infrastructure assets, systems, and networks that it depends on for normal day-to-day operations. These connections, or dependencies, may be geographically limited or span great distances (*NIPP 2013*). The many points of infrastructure connections, and their geographic distribution, make the infrastructure environment much more complex. The U.S. Department of Homeland Security (DHS) works to strengthen critical infrastructure security and resilience by generating greater understanding and action across a (largely) voluntary partnership landscape. This is achieved by working with private and public infrastructure stakeholders to resolve infrastructure security and resilience knowledge gaps, inform infrastructure risk management decisions, identify resilience-building opportunities and strategies, and improve information sharing among stakeholders through a collaborative partnership approach. This paper highlights the Department's efforts to present a more comprehensive picture of security and resilience through a "system of systems" approach.

1 INTRODUCTION

The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across the government and the private sector. IP conducts and facilitates vulnerability assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners manage risks to critical infrastructure. Effective risk management requires an understanding of dependencies and interdependencies of infrastructure (*NIPP 2013*). IP has demonstrated experience in analyzing critical infrastructure dependencies and interdependencies at a regional level. Since 2009, IP has led the Regional Resiliency Assessment Program (RRAP), a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure that is regionally and nationally significant. The goal of these voluntary, non-regulatory resiliency assessment projects is to generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure.

Strong partnerships with Federal, State, local, tribal, and territorial government officials and private sector organizations across multiple disciplines are essential for the success of these projects. Key partnerships include private sector facility owners and operators, industry organizations, emergency response and recovery organizations, utility providers, transportation agencies and authorities, planning commissions, law enforcement, academic institutions, and research centers. These assessments typically involve a year-long process to collect and analyze data on the critical infrastructure within the designated area, followed by continued technical assistance to enhance the infrastructure's resilience. Each assessment can incorporate opportunities for valuable information and data exchanges, including voluntary facility security surveys, first responder capability assessments, targeted studies and modeling, and subject matter expert workshops. The culmination of assessment activities, research, and analysis is presented in a

summary report documenting project results and findings, including key regional resilience gaps and options for addressing these shortfalls. Partners can use the results to help guide strategic investments in equipment, planning, training, and infrastructure development to enhance the resilience and security of facilities, surrounding communities, and entire regions.

2 METHODOLOGY

2.1 Overview

Infrastructure dependency and interdependency analysis can be analytically complicated, time-consuming, and costly, which, in turn, can limit stakeholders' ability to understand and use this information to make risk-informed decisions that enhance resilience. To manage these complexities, IP applies a process that helps partners prioritize resilience assessment efforts by adopting a "system of systems" approach to regional dependency and interdependency analysis. This approach is based on the assumption that a critical asset or facility can be considered as part of a broader system of infrastructure. Higher-level constructs (e.g., a community or a region) include multiple systems. As such, a community or a region operates as a "system of systems." Viewed within this framework, high-level systems analysis—using proven and scientifically sound tools—can help identify the most critical lower-level systems. This information, in turn, can help determine where to conduct more detailed site assessments, focusing only on the most critical asset-level components (Carlson et al. 2012).

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 (Carlson et al. 2012). Using this approach, analysis would consider the high-level context (e.g., a geographic region or 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. Executing this "system of systems" approach to fully consider regional infrastructure dependencies and interdependencies requires the application of system science methodologies and a combination of top-down and bottom-up data collection and analysis methods. Dependencies and interdependencies exist at individual levels i.e., assets are interconnected with other assets) and between levels (i.e., assets are interconnected with systems, systems with other systems, and so on).

Assessing infrastructure dependencies and interdependencies to improve regional resilience requires a scalable approach that can be tailored based on decision support needs, stakeholder requirements, and relevant critical infrastructure. Performing dependency and interdependency analyses is not a one-size-fits-all activity. Stakeholder goals, available data, time, budget, and analytical sophistication all combine to influence the scope and complexity of potential dependency analysis. Thus, the core concept of the framework outlined here is to establish a flexible approach that covers a broad spectrum of options, starting with relatively simple and tightly scoped efforts and culminating in more complex, integrated evaluations.

Data collection tools and analytic methodologies are expanding from traditional evaluations of physical dependencies to include cyber and geographic dependencies, as well as visualizations of first-order cascading failures. However, many existing tools and models operate in silos. Over time, more advanced infrastructure interdependency analysis can consider all dimensions of critical infrastructure dependencies and interdependencies, including operating environment, coupling and response behaviors, types of failure, infrastructure characteristics, and state of operations (Petit et al. 2015). These advanced approaches require new data-collection mechanisms and the integration of independent, but complementary, tools and models. The more advanced analysis enables stakeholders in public and private sectors to move from traditional analysis—centered on individual facilities—to broader systems-level evaluations of infrastructure dependencies and interdependencies and identification of key failure points

The "system of systems" approach focuses primarily on the assessments of interconnections between the regional functions of focus (e.g., critical manufacturing, public health, etc.) and lifeline sector systems of interest (e.g., energy, communications, water, wastewater, and transportation). The objective of this process is to characterize the vulnerability and resilience of key systems and lifeline sectors and to better understand how existing dependencies and interdependencies could generate cascading or escalating failures. The subsequent sections outlines the general approach applied by IP to understand infrastructure interdependencies.

Figure 1: Infrastructure interdependency assessment phases.

2.2 Identify Stakeholder Needs

Defining the primary stakeholders (including Federal, State, and local partners and key private sector partners), their requirements, and the information they need to make decisions is a first step in conducting infrastructure interdependency analysis. A solid understanding of the information needs of makers and the business processes in which these decisions occur is essential to scoping the critical infrastructure systems for assessment and the required level of analysis, particularly because interdependency assessments of critical infrastructure can be tailored to different levels (e.g., asset, system, network, or functions).

This phase may involve an initial review of existing documentation (e.g., previous assessments and characterizations of infrastructure, existing plans, GIS data, and other available information) to refine the project scope and identify a preliminary list of systems and assets that enable the regional function of concern. This phase also involves coordination with the other Federal, State, and local governance structures in place to oversee preparedness, mitigations, response, and recovery efforts.

2.3 Identify Important Regional Functions and Infrastructure Systems of Concern

The next phase centers on identifying the infrastructure sector or system within the geographic area and defining the most critical assets (including those in systems of focus, as well as nodes and links in lifeline infrastructure systems) that would have detrimental security, economic or social impacts if disrupted. During this phase, IP analyzes, revises, and prioritizes the preliminary lists of assets and utility nodes, based on input from private and public sectors, as well as critical infrastructure owners and operators.

2.4 Collect System and Asset-level Data

This third phase involves gathering qualitative and quantitative data to characterize the systems of focus and lifeline infrastructure systems identified during Phase 2. This may include reviewing existing data that had been collected, compiled, and/or analyzed (e.g., databases, GIS layers, reports, best practices), or may necessitate site visits to selected facilities and infrastructure assets. During this time, analysts meet with infrastructure operators to learn about the facility's operations, potential impacts from disruptions to supporting lifeline infrastructure, and existing security and emergency procedures. The meetings often include a physical tour of the facility for a general understanding of facility operations and to observe the protective and resilience measures in place, as well as the utility connections. During site visits, dependency surveys and structured interviews are used to collect standardized information across facilities to assess the impacts of a disruption or loss of utility services on an asset's operations and a system or asset's essential

functions. These discussions are intended to uncover operational characteristics of relevant infrastructure owners and operators and their role in potential cascading and escalating failures.

The data-collection phase may necessitate the development of a data architecture and data dictionary to enable analysts to understand the completeness of available data, support system-level modeling and analysis, and identify opportunities for future engagement with public and private sector partners involved in interdependency analysis.

2.5 Analyze Infrastructure Dependencies

This phase is the core of the assessment approach, during which subject matter experts analyze the data collected for two categories of infrastructure: Infrastructure critical to systems or sectors of concern; and Lifeline infrastructure providing essential resources and services to the system or sector of concern. The assessment will typically addresses energy, communications, water and wastewater systems, and transportation systems.

The interdependency analysis process requires top-down and bottom-up approaches to characterize infrastructure connectivity within and across sectors. Top-down dependencies analysis involves empirical-based, network-based, and system dynamic-based approaches to estimate the service capabilities of infrastructure systems (table 1-4). Empirical approaches are grounded in real-world observation of failure patterns. The network-based approach hinges on identifying critical utility nodes and their functions and then identifying potential resilience enhancements. This approach captures key characteristics (e.g., flows, operational mechanisms) of lifeline infrastructure sectors. The system dynamics-based approach complements the network-based approach by modeling the effect that the operating environment has on lifeline infrastructure system functions. It helps capture the effects of policy and technical factors that drive infrastructure system evolution.

Bottom-up analysis of infrastructure dependencies focuses on understanding the needs of critical systems and utility assets for specific infrastructure resources (e.g., electricity, fuels, water, wastewater, communications, and critical supplies). The focus is on impacts of a disruption to these resources and services at a specific facility. Data collection focuses on framing the variation in facility performance over time in light of these disruptions, including timelines, extent, and duration of the loss of services; measures in place (e.g., procedures, backup) to mitigate loss; and the extent of overall degradation on a facility's operations. Analysts collect this information at a subset of facilities in the region based on time and accessibility, create a standardized structure through which to collect the information at other facilities in the future, and integrate this information into a broader data architecture to support analysis and visualization.

Top-down and bottom-up dependency analyses can be combined to define a high-level abstraction of infrastructure interdependencies that allows analysts to anticipate potential cascading and escalating failures within and across sectors. Each critical system and utility is visualized as a layer based on top-down dependency analysis. For example, top-down dependency analysis of the electric grid shows how the disruption of given nodes or links (e.g., generator, line, or substation) or several nodes and links (e.g., n-2 contingency studies) would propagate across the electric grid and generate outage areas. Bottom-up analysis characterizes how operations at facilities within the power outage areas would be impacted. This use of "system of systems" interdependency analysis sheds light on downstream cascading and escalating failures. However, the approach also informs upstream analysis about how utility systems supply critical resources to a specific area of interest.

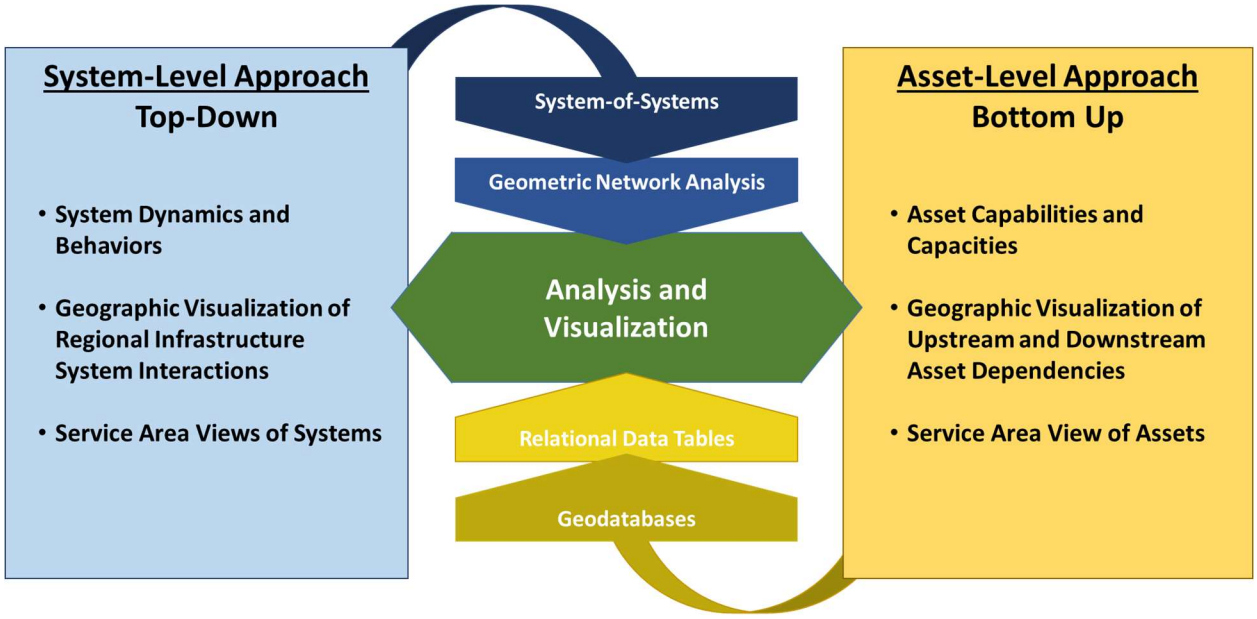

Figure 2: A system-of-systems visualization abstraction.

2.6 Develop Tools and Final Products

These assessments produce Summary Reports, which document project results and findings, including key regional resilience gaps and options for addressing these shortfalls. IP provides the report, along with supporting documents and information, to select assessment participants in the form of a multimedia presentation. Facility owners and operators, regional organizations, and government agencies can use the results to help guide strategic investments in equipment, planning, training, and infrastructure development to enhance the resilience and security of facilities, surrounding communities, and entire regions. Assessments will also frequently result in the development and delivery of Decision Support and Analytic Resources Tools. These outputs are intended to support situational awareness or may support the implementation of resilience enhancement measures identified during the course of the assessment, and may include detailed GIS maps, geocoded databases, graphical products, facility reference documents, and other resources to enable the continuation or expansion of the resiliency assessment.

3 INFRASTRUCTURE SYSTEM CHARACTERIZATION

Interdependencies among lifeline infrastructure systems continue to grow in number and complexity, resulting in systems that are increasingly vulnerable to cascading and escalating effects across infrastructure sectors. Infrastructure owners and operators, as well as customer bases for their services and resources, increasingly seek an enhanced understanding of interdependencies among infrastructure systems—including both the vulnerabilities and opportunities that these relationships produce—to anticipate and respond to the potential effects from a change in system dynamics. These issues are equally pertinent to post-incident recovery plans and programs, where public and private sector partners make investment decisions on rebuilding infrastructure to be more resilient to a range of threats and hazards.

Top-down approaches to infrastructure analysis center on assessing and characterizing infrastructure systems, conducting modeling and failure analyses at the system level, and ultimately integrating these efforts into system-of-systems analyses that hone in on critical nodes across systems that can lead to cascading and escalating effects.

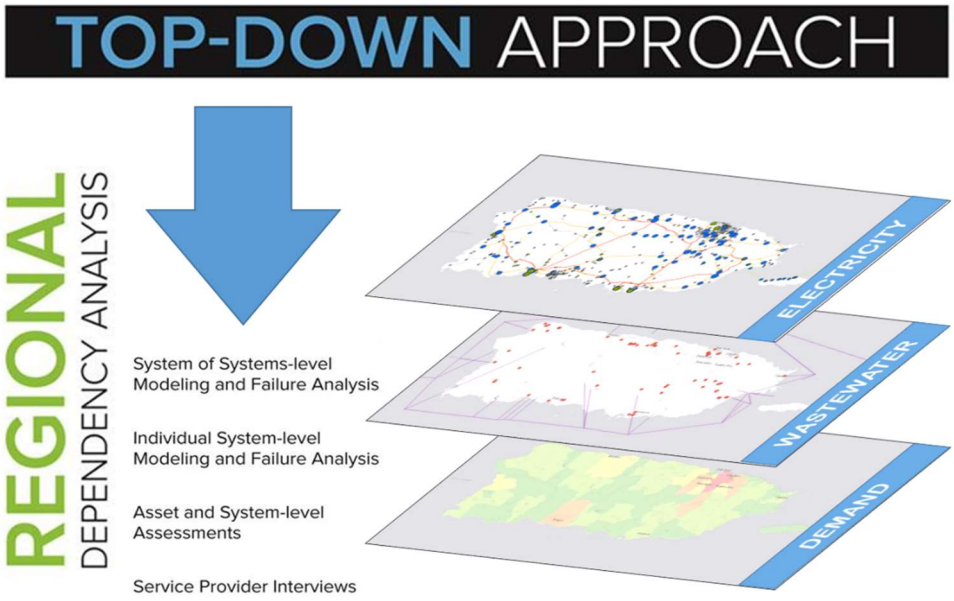

Figure 3: Focusing on top-down dependencies.

One foundational component of top-down, system-level analysis is the process of characterizing infrastructure sectors of interest. This process includes defining how the system functions in general, how it functions in a particular geographical and operational context, the interdependencies between that sector and other critical infrastructure systems, and the potential consequences that could result from cascading failures. Characterizations include a mix of operational information (i.e., to understand functions and capacities of system components) and geographic data (i.e., GIS information that visualizes systems within a given geographic footprint). These initial system characterizations are the basic building blocks for more advanced analysis that uses these inputs in models and simulations.

For IP's resiliency assessments, the goals of infrastructure interdependency analysis includes the following: (1) characterizing the vital hubs and chains of activity for key sectors and their dependencies on lifeline infrastructure and (2) mapping and analyzing the dependencies and interdependencies between these users and the infrastructure, as well as between infrastructure sectors themselves. Therefore, a key initial step is to identify which infrastructure sectors and subsectors to characterize, with an eye toward integrating that information with asset-level data collected through a bottom-up process running in parallel for key infrastructure systems. Lifeline critical infrastructure sectors and subsectors are consistently focal points for system-level analysis during these assessments.

Several modeling and simulation approaches, generally developed for risk assessment and system engineering, also apply to critical infrastructure interdependencies analysis. Three categories are particularly relevant: empirical-based, network-based, and system dynamics-based.

Table 1: Modeling and Simulation Approaches.

Approach	Description
Empirical-Based	Analyze interdependencies based on observation and experience by using historical data in combination with expert judgment.
Network-Based	Analyze infrastructure systems as networks where infrastructure assets are represented as nodes and the physical connections are represented as arcs.

System Dynamics-Based	Analyze the behavior of complex systems by modeling a system's dynamic and evolutionary behavior through stock and flow exchanges and causal loops.

When sequenced and integrated during a resiliency assessment, these approaches can help public and private sector partners identify the different functions within the lifeline system and identify the physical assets that enable the system to perform its required functions. This in turn enables an understanding of how the failure of physical assets would propagate within the system; and can provide infrastructure partners with investment justification for the implementation of protective and mitigation measures.

4 INFRASTRUCTURE ASSET CHARACTERIZATION

Lifeline infrastructure assets are interconnected and mutually dependent in multifaceted ways. Understanding the full extent of dependencies and interdependencies among infrastructure assets is essential to developing resilience strategies that mitigate the potential for cascading and escalating impacts to the communities and industries that depend on these assets (Clifford and Macal 2012). Bottom-up analysis of infrastructure dependencies estimates the needs of infrastructure assets for specific resources. Data collection focuses on capturing the characteristics and performance of specific downstream users of infrastructure and the upstream infrastructure assets that provide critical services and resources

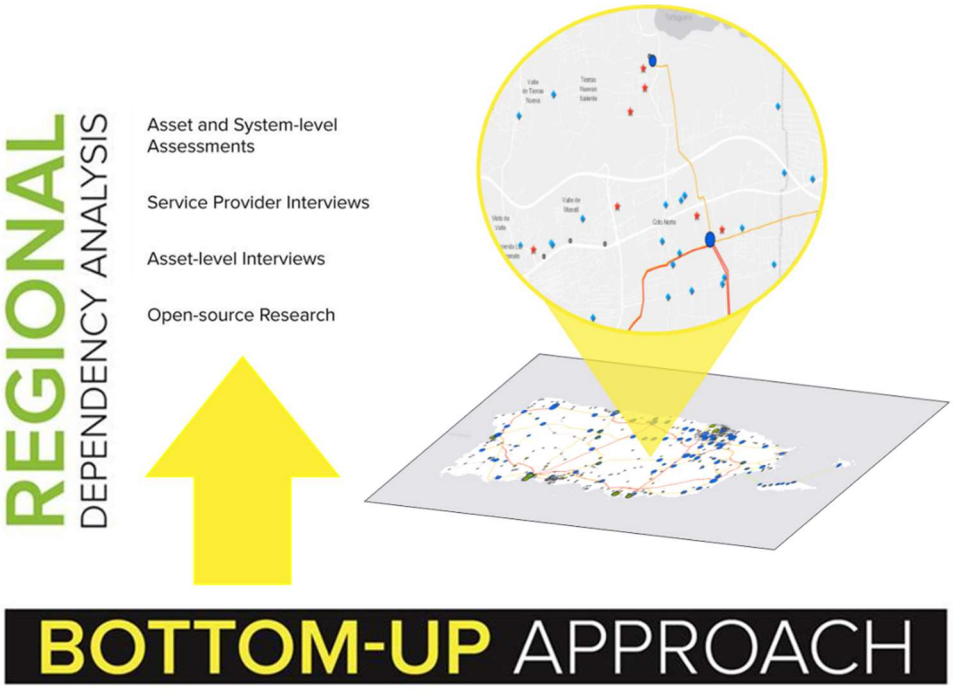

Figure 4: Focusing on bottom-up dependencies.

The focus of the bottom-up approach is on the potential downstream effects of a change in upstream operations. An infrastructure asset is considered to be "upstream" from entities to which it provides services or resources. The recipients of those services or resources are therefore "downstream," and may include both users of infrastructure such as manufacturing facilities as well as other infrastructure assets.

Connections between users of infrastructure and the infrastructure assets may also be direct or indirect. A first-order dependency describes a relationship in which an infrastructure asset provides a direct service or resource to a user. This provision could be through a specific connection, such as a distribution substation and line, by which the operation of the infrastructure asset will have an immediate impact on its user.

A second-order dependency describes a relationship in which an infrastructure asset indirectly supports the operations of a downstream user. These include the upstream interactions between infrastructure assets, one or both of which provide direct services or resources to a user. The operation of the one infrastructure asset may therefore affect the operations of another, propagating an effect to all downstream users. Figure 3-3 illustrates a notional example of the second-order dependencies of a facility of interest (e.g., a pharmaceutical manufacturer) that result from the facility's first-order dependency on electric power.

5 CONCLUSION

IP has conducted resiliency assessments across the United States for more than a decade, completing over 80 regional resiliency assessment projects and leveraging its dependency analysis framework to support various infrastructure planning, response, and recovery efforts with partners across the Nation. This experience has enabled IP to develop, implement, and refine its infrastructure resiliency assessment approach and dependency analysis framework, and improve its ability to identify opportunities to enhance regional critical infrastructure security and resilience.

IP has consistently observed several important themes related to infrastructure resilience. First, there is a widespread lack of visibility or understanding of how critical infrastructure components are interconnected and how systems are dependent or interdependent on one another. This is reflected in the response and recovery plans, which seldom include all relevant stakeholders or address known hazards in a comprehensive manner. Second, a lack of redundancy, insufficient system capacity, or both, diminishes the resilience of many infrastructure systems. Many critical assets and systems pursue multiple connections to lifeline infrastructure in order to offset the potential consequences of losing service through a single connection. Related to this challenge, a lack of diversity in available options may result in critical dependencies on infrastructure assets that are potential single points of failure during emergencies. A dependence on energy, aggravated by an insufficiency of back-up power systems, is the most pervasive resilience gap noted in resiliency assessments (Bowman 2016). Developing a better understanding of infrastructure dependencies and enhancing coordination across partners is the first step in addressing these challenges. Nearly all infrastructure partners and stakeholders – governments, industries, and utilities – would benefit from a greater level of coordination and information sharing, especially at the regional and cross-regional level.

The lessons learned from IP's resiliency assessments emphasize the importance of approaching resilience from functional, systems-based orientation. There is a broad need to think, design, and plan in terms of tiered levels of function and acceptable timelines for restoring functions in response to a disruption, but also a need for the ability to approach resilience in a hazard-agnostic fashion.

IP has worked to identify and explore resilience gaps and the conditions that create them. Sharing these findings with relevant infrastructure partners and stakeholders not only enhances their understanding of interdependent system operations, it also enables them to take action to address potential gaps and shortfalls. IP will continue to advance its understanding of critical infrastructure security and resilience through the application and evolution of its resiliency assessment approach. Doing so will not only lead to the development of a deeper understanding of critical infrastructure systems, but also enable our public and private sector partners by providing them with the tools, methodologies, and common themes necessary to take action.

ACKNOWLEDGMENTS

The author wishes to acknowledge its partners at Argonne National Laboratory and Idaho National Laboratory for supporting the development and implementation of the Dependency Analysis Framework and the Regional Resiliency Assessment Program.

REFERENCES

The United States Department of Homeland Security. 2013. *National Infrastructure Protection Plan (NIPP), Partnering for Critical Infrastructure Security and Resilience.*

Carlson, L., G. Basset, W. Buehring, M. Collins, S. Folga, R. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitefield. 2012. *Resilience Theory and Applications*, Argonne, Illinois: Argonne National Laboratory, Decision and Information Sciences Division.

Petit, F., D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom. 2015. *Analysis f Critical Dependencies and Interdependencies*. Argonne, Illinois: Argonne National Laboratory, Global Security Sciences Division.

Clifford, M. and C. Macal. 2016. *Advancing Infrastructure Dependency and Interdependency Modeling: A Summary Report from the Technical Exchange*. Argonne, Illinois: Argonne National Laboratory

Bowman, R. 2016. *Strengthening Critical Infrastructure Resilience by Identifying and Redressing Recurring Gaps and Systemic Barriers; Lessons from a Cross-Case Analysis and Synthesis of the U.S. Department of Homeland Security Regional Resilience Assessment Program*. Boston, Massachusetts: Northeastern University.

AUTHOR BIOGRAPHIES

SCOTT BREOR currently serves as the Deputy Assistant Secretary (Acting) for the Office of Infrastructure Protection (IP) within the U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), where he helps oversee IP's efforts to help secure the nation's critical infrastructure. Previously, Mr. Breor served as the Director of IP's Protective Security Coordination Division (PSCD), where he oversaw a nationwide cadre of critical infrastructure security specialists known as Protective Security Advisors (PSAs). He also led the division's efforts in vulnerability and security gap analysis; support to special events; and training on topics including active shooter preparedness; suspicious activity reporting; and improvised explosive device (IED) awareness and bomb threat management. Mr. Breor has over thirty years of military and senior executive experience in the United States government. Prior to DHS, Mr. Breor was a Naval Aviator and had served as the Senior Policy Advisor for the Chief of Naval Operations on all Homeland Security matters. While assigned to the Office of the Chief of Naval Operations (CNO) he led a division that supported the CNO on key warfare and Homeland Security and Defense policy decisions, which included: interagency coordination, incident management, and Department of Homeland Security/Department of Defense integration. For his work for the CNO and his efforts following the tragic events of September 11, 2001 at the Pentagon, he was awarded the Legion of Merit. As a Naval Aviator he supported operations in Iceland, Greenland, Adriatic, Mediterranean, Azores, and South America. Mr. Breor was a Senior Executive Fellow at the John F. Kennedy School of Government, Harvard University. He received a Masters of Arts in National Security Studies and in Homeland Security and Defense from the Naval Post Graduate School, and received a Masters of Business Administration from the University of Oklahoma. In addition, he earned a Bachelor of Science in Physics from The Citadel.