Interconnected Risks in Electricity Systems: Understanding Research Challenges, Needs, and Partnerships

Heidi Applegate, Bobby Jeffers, Ryan Burg,
Cameron Friday, Laura Leddy, Sara Peterson,
Maurice Martin, and Eliza Hotchkiss

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-90869
January 2025

Interconnected Risks in Electricity Systems: Understanding Research Challenges, Needs, and Partnerships

Heidi Applegate, Bobby Jeffers, Ryan Burg,
Cameron Friday, Laura Leddy, Sara Peterson,
Maurice Martin, and Eliza Hotchkiss

National Renewable Energy Laboratory

Suggested Citation
Applegate, Heidi, Bobby Jeffers, Ryan Burg, Cameron Friday, Laura Leddy, Sara Peterson, Maurice Martin, and Eliza Hotchkiss. 2025. *Interconnected Risks in Electricity Systems: Understanding Research Challenges, Needs, and Partnerships*. Golden, CO: National Renewable Energy Laboratory. NREL/TP- 5R00-90869. https://www.nrel.gov/docs/fy25osti/90869.pdf.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-90869
January 2025

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the National Renewable Energy Laboratory. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Acknowledgments

NREL thanks workshop participants and planners and acknowledges external participants who dedicated time to travel to Golden, Colorado, to share their views and actively engage in discussions. Participants came from utilities, industry, government offices, research organizations and national laboratories.

This 2-day workshop was funded by NREL’s Energy Security and Resilience Program Office as part of an effort to understand the opportunities for collaboration across industry, government agencies, utilities, research organizations, and DOE laboratories to address risks associated with the electricity system.

Table of Contents

1 Background

The United States faces formidable challenges in simultaneously mitigating short-term emissions, adapting to long-term climate change risks, ensuring energy security, and confronting escalating threats of attacks to critical infrastructure. These challenges constitute a diverse, interdependent, and complex risk landscape for the U.S. electricity system. Mitigating interconnected risks requires both long-term planning and rapid operational response—capabilities that require investment and collaboration to develop and maintain. However, given the rapid pace of change in the electricity system's risk environment (see Figure 1), it is increasingly difficult for markets, regulatory processes, and professional groups to adapt. In some cases, it is not clear who will bear the costs of new risks nor how these costs can be recovered in energy markets. Without well-informed policy and funding, risk mitigation strategies remain poorly integrated within many dominant infrastructure planning paradigms.

The U.S. federal government and its research organizations have a potential role in mitigating the most poorly addressed risks across electricity markets and interdependent systems. Electricity system risks stem from extreme acute shocks (e.g., cyberattacks, extreme weather, and supply chain disruptions) and chronic stressors (e.g., global economic competition, uncertainties surrounding emerging technologies, climate change, and related conflicts). These acute shocks and chronic stressors can result in dire consequences for society, underscoring the need for more predictive and complete information for decision makers in both public and private sectors. To deliver this information, improved approaches to risk quantification and risk management must be rapidly developed and disseminated, ultimately leading to best practices and standardization. Informed by a quantitative treatment of risk to electrical infrastructure and interdependent systems, decision makers can more prudently and efficiently prioritize mitigation initiatives to maximize benefits to government, businesses, and the public.

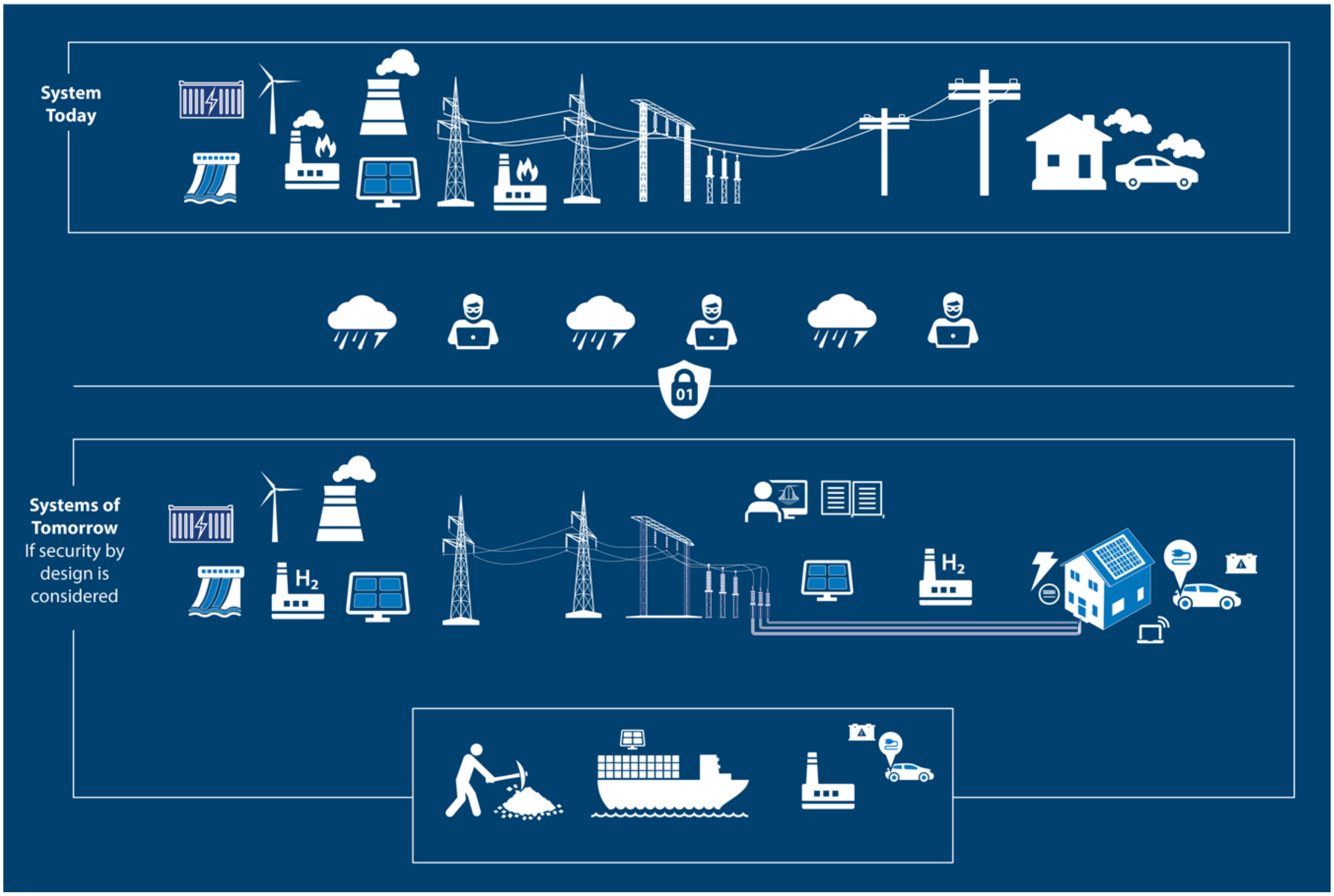

Figure 1. The energy system of tomorrow

Image by Anthony Castellano, National Renewable Energy Laboratory (NREL)

2 Workshop Purpose and Structure

2.1 Purpose

The purpose of the Electricity System Risk Quantification Workshop was to help identify the most pressing risk quantification gaps requiring deliberate, robust, and coordinated research from the U.S. Department of Energy (DOE) national laboratories and their partners. Addressing these challenges will help support decision-making and lead to improved resilience and security investments in the national interest, thereby reducing the negative consequences to our society associated with power interruptions, price spikes, or energy availability issues (see Figure 2).

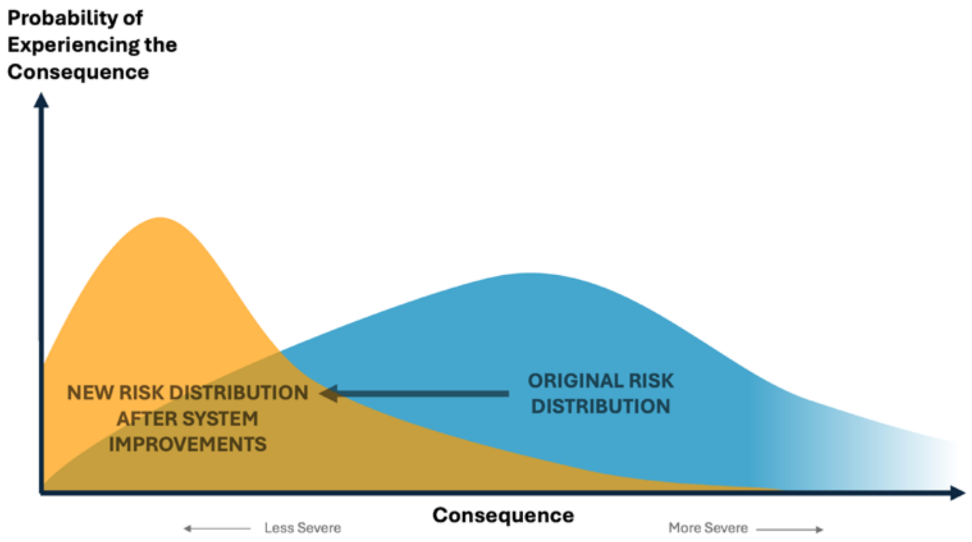

Figure 2. Reducing risk consequence

Image by Cameron Friday, National Renewable Energy Laboratory (NREL)

2.2 Structure

The workshop was structured around challenges in electricity system risk quantification, including three subtopics: consequence quantification, vulnerability assessment and identification, and hazard/threat characterization (see Table 1). These three subtopics also form a classic equation for risk, allowing decomposition of complex challenges:

Risk = Threat x Vulnerability x Consequence

Three panel discussions—one for each subtopic—provided initial context for smaller group conversations on knowledge gaps; data, modeling, and procedural needs; and partnerships most critical to each subtopic. Small groups shared their findings through plenary discussions, during which participants voted to identify the most pressing challenges for each subtopic.

The workshop concluded with a final plenary to synthesize main themes, prioritize needs, and identify additional stakeholders. The workshop spanned all scales of input and analysis—from individual households to the nation as a whole—and needs ranging from data and modeling to convening functions.

Table 1. Definitions and Key Questions

Subtopic	Definition	Key Questions
Consequences	Consequences of a disturbance include both human and national security impacts as well as the multi-stakeholder costs and benefits of restoration and recovery.	What consequences and mitigation costs of energy system disruptions are not aligned? Where is the line between a public good and a private good for resilience and security?
Vulnerabilities	Vulnerabilities are weaknesses within infrastructure, systems, or processes that, when exposed to hazardous conditions, increase the likelihood infrastructure will fail and the extent to which it will fail to deliver its intended service.	Which aspects of vulnerability assessments must be improved to mitigate the risks the group identified during the consequences breakout? What makes vulnerability assessments challenging? How do we improve on vulnerability assessment practices?
Hazards and Threats	Hazards and threats expose a vulnerability or damage, destroy, or disrupt an asset. The terms “hazards” and “threats” may be used interchangeably, although some sources consider threats a subcategory of hazards, referring specifically to human-caused incidents.	What are the hazards and threats most in need of improved characterization for a sufficient risk assessment?

Participants shared their observations during the panels, small groups, and plenary sessions, yielding an extensive list of challenges, needs, stakeholders, and contextual comments related to electricity system risk quantification. Discussion on the technical needs supporting an understanding of the threats often flowed into vulnerabilities and consequences and vice versa. Moreover, participants noted the complexity, fluidity, and interconnection of issues across the categories of threat, vulnerability, and consequence, where some of the issues were viewed as crosscutting or supporting a broader risk quantification and risk management paradigm.

3 Challenges and Needs

NREL staff synthesized content from the workshop's breakout conversations and plenary discussions into key challenges and associated needs. Recurring topics throughout the workshop included interdependencies and the need for cross-functional teams and decision-making support. Many participants identified risk quantification challenges related to their domains of expertise in which the challenges were most apparent to them. They were less aware of risk quantification challenges outside their own domain (e.g., the challenges of risk quantification within cybersecurity may not be apparent to climate risk specialists and vice versa). In addition, key challenges of varying levels of specificity were identified. These key challenges have further been categorized into "Core Challenges," which are complex and multifaceted, and "Compounding Challenges," which may be inherently less complicated but add to the difficulties of understanding and identifying solutions to the Core Challenges.

3.1 Core Challenges and Related Needs

Challenge: There is no unified or universally embraced framework for electricity system risk quantification and comparison of risks across domains, making risk prioritization difficult.

What is at stake? Insurance, market valuation, access to capital, and regulatory approaches depend on a shared understanding of higher-order, shared, systemic regional and national-scale risk and the incidence of these risks within the electrical system. Some types of risk, such as rare events in the "tails" of the distribution, are also highly reliant on public sector action because investments in mitigating these risks are non-excludable goods. Goods that are non-excludable produce benefits for third parties without providing an easy mechanism to recover the cost of providing these benefits to these third parties. Non-excludability is often recognized as a key aspect of the kinds of public goods that are financed with public sector resources. For example, defense against an interconnect-wide, month-long outage should apply to every citizen equally without exclusion because on these scales, electricity is fundamental to human health and wellbeing. These three features – a dependence on shared understanding, a need for regulatory action, and an element of public good within the risk – mean that government at all levels has a core role to play in creating a framework for risk quantification, and understanding where their policy, regulatory, and service provision roles apply within the framework.

If quantification methodologies are undeveloped, underdeveloped, or divergent, they may unintentionally intensify a sense of uncertainty and a perception of unmanaged risk in the sector. By contrast, a methodology that quantifies uncertainty across scenarios should help solidify a shared understanding of risk management, facilitate coordination and collaboration, to inform policy, planning and to improve the performance of existing governance mechanisms, such as securities regulations and ratings methodologies.

Needs in this area include the following:

- Publicly available, standardized methodology and terminology for cross-domain electricity system risk calculation that incorporates risks to the economy and to the pace of change within the sector itself.
- A more explicit connection between a standardized risk methodology and the decisions by various parties, including government at all levels, that will create a more efficient market for buying down these risks.
- Better data management and communication
- Clear guidelines for and best practices in risk quantification
- Increased collaboration between institutions, government, and stakeholders (narrow/siloed thinking identified as a major risk)
- More consistency/translation between the proliferation of different models in this space (e.g., utilities, states, insurance), including a framework approach links existing risk models
- Locational, event-type-specific fragility curves for vulnerability assessments.
- Domain-specific approaches to risk quantification as applicable to complex sub-systems and their interactions, e.g. water-energy nexus, food security.

Challenge: Uncertainty and complexity are treated inconsistently if at all, and it is not well communicated in support of decision making under uncertainty.

What is at stake? Without a clear explanation of the degree of uncertainty in risk estimates, decision makers may place undue emphasis on some elements of risks over others that warrant consideration. This is especially apparent for tail risks and those which involve inherent interdependencies and complex interactions across systems. Furthermore, communication of uncertainty and complexity can send a signal that electricity system stakeholders lack a clear picture of the future, leading to these types of risks being underrepresented or altogether ignored. Without a consistent and robust treatment of uncertainty and complexity, decisions are being made focused on risks that are easier to quantify and more certain, leading to a brittle system that targets reliability above resilience, short-term payoff over long-term gain, and consolidated private benefit over dispersed public benefit.

Uncertainty quantification, complexity management, and communication techniques provide a barometer for risk quantification to better track the maturation of risk management over time. Given the number of potential pitfalls in the energy transition and the diversity of entities impacted by them, there is significant value in procedures to estimate the range and magnitude of these risks.

Needs in this area include the following:

- Consistently applied uncertainty and confidence management terminology and methods
- Purposeful attention to complexity and utilization of complexity management techniques when addressing interconnected or interdependent risks.
- Maturation of approaches to communicating uncertainty and complexity, with attention toward common human fallacies in this space

- Frameworks and standardized approaches for integrating relevant real-world data into sensitivity analysis
- Methods to enable uncertainty quantification into all risk analysis, including mitigation assessments and cybersecurity evaluation.

Challenge: There is an insufficient ability to model the interdependent nature of human infrastructure and supply chains.

What is at stake? Because risks can cascade through complex causal pathways, downstream consequences of a seemingly isolated event can rapidly increase. Although it may not be possible to determine which events will have the most pronounced downstream impact, estimating the average extent of these possible impacts may help increase the expected value of nontargeted, grid-wide mitigations.

Needs in this area include the following:

- Better information sharing across entities in the energy security landscape (e.g., utilities, local/state/federal governments, regulatory agencies, institutions)
- More research for understanding the increasingly complex global supply chain for materials used in renewable energy technologies
- Better modeling of the nonlinear relationship between the duration and impact of energy disruptions.

Challenge: Energy resilience and security data are inherently sensitive, which creates a paradoxical situation with broader data sharing: The more data are shared, the more a potential vulnerability is created for attackers to target.

What is at stake? Key initiatives in grid governance focus on increased transparency in grid configuration and operation. Likewise, sharing information on gaps in appropriate risk management could encourage good behavior in mitigating these risks. However, inherent transparency and transparency regarding gaps in risk management can provide additional strategic information to threat actors and potentially magnify threat consequences. What results is a paradox of transparency: the very openness required to justify and govern risk mitigation investments may also invite additional and better-targeted attacks.

Needs in this area include the following:

- Synthetic infrastructure data—data created by artificial intelligence models trained on real-world data samples—to support risk-modeling efforts when entities are not willing or able to share actual data
- Frameworks and approaches for considering the threat of domestic extremists who have ample information (especially when compounded by the unavailability of supply chains to remedy physical attacks)
- Novel approaches for data sharing that protect critical information (especially the critical nature of specific places) as more stakeholders engage in the conversation.

Challenge: Mitigation costs for low-probability events are hard to justify before an event happens. It is easy to underestimate the need for resilience, and it is difficult to motivate investments in resilience.

What is at stake? Funding for resilience mitigation depends on a recognition of effective risk mitigation and a broad awareness of risk mitigation activities and their limitations. Furthermore, funding depends on clear roles across public and private stakeholders. Common understanding of the set of roles and responsibilities for buying down these risks is not shared.

Needs in this area include the following:

- A clear set of priorities, regulations, and standards for infrastructure performance that can be used to motivate or incentivize investments in resilience
- Frameworks for prioritization of risks across different areas (e.g., natural gas, renewable energy generation, and nuclear from a utility perspective)
- Better quantification and communication of uncertainty in low-probability events.

Challenge: The climate change implications for energy security and resilience are not certain or clear.

What is at stake? Integrating climate model outputs and incorporating climate risk into grid-planning practices are critical. These practical steps depend on more clarity in the use of scenarios and the long-term dynamics with other complex processes such as migration, global supply chain stability, and international conflict.

Needs in this area include the following:

- Communication of threats and hazards, vulnerability, and consequences in the context of rapid change, considering potential future trajectories rather than the status quo
- Improved capacity to model (and to interpret models) in ways that can inform resilience investments—perhaps by relying on worst-case scenarios rather than “typical” scenarios.
- Coordination between climate risk modeling and economic risk modeling to accurately assess the costs and benefits of resilience investments that yield adaptations for future grid performance.

3.2 Compounding Challenges and Related Needs

Challenge: Accountability is not always transparent or borne by those who will benefit from action. Requests or demands for mitigation are often not brought to the stakeholders who would play a role in the mitigation.

What is at stake? Without a coherent allocation of responsibility, the “politics of blame” may impose obligations on entities that are neither funded nor empowered to take appropriate mitigating actions. This uncertainty is exacerbated by cost risk. Cost uncertainty poses risk in both risk mitigation and consequence estimation, where the magnitude of major event recovery costs is difficult to estimate, as is the real cost of resilience. These uncertainties can shape and inhibit funding options.

Needs in this area include the following:

- A list of stakeholders involved in energy resilience and energy resilience domains such as cybersecurity and climate adaptation
- A list of functions that these stakeholders and their organizations perform
- A matrix of stakeholders and functions indicating which stakeholders could take on which functions
- A system for assigning functions to stakeholders
- Metrics for asserting stakeholders have fulfilled their assigned functions
- More clarity in funding options for risk mitigation.

Challenge: Research organizations in support of various stakeholders in the electricity system largely do not have a full picture of the data they need, and they certainly do not have it.

What is at stake? Risk models are inherently informed by specialized datasets. Without a comprehensive inventory of these datasets and the associated needs that they meet, risk quantification will continue to struggle with key risk elements.

Needs in this area include the following:

- More coordination of data gathering efforts across stakeholders:
    - Utilities
    - Federal agencies
    - State and local decision makers
    - National laboratories
    - Research institutes and universities
    - Industry partners
- Data on low-probability, high-impact events (perhaps synthetic data to supplement limited real-world datasets)
- Artificial intelligence/automated approaches to aggregate and interpret the vast quantity of data.
- What about the technology to manage privacy of the date?

Challenge: Visibility is poor into the combined cybersecurity risk associated with a proliferation of new smart grid stakeholders.

What is at stake? With increasing internet connectivity at the grid edge and increasing real-time operational aggregation—an increasing number of devices such as smart inverters and electric vehicles interacting in ways that add up to a substantial instantaneous force on the power grid—electrical system risk from cybersecurity disruption can have significant implications for individual customers and at higher levels of aggregation.

Needs in this area include the following:

- Help with identifying and prioritizing specific cyber risks most associated with significant business consequences
- Development of risk registers (i.e., What are the common cyber scenarios we are all facing?)
- Crown Jewel Analysis, a methodology to identify mission critical cyber assets
- Open-source cyber risk quantification model
- Consistent, transparent approach across the industry to build customer trust and avoid accusations of pushing unnecessary or proprietary mitigations
- Simulation model that can parse nondisclosed data in a consistent manner so that simulation results can be interpreted and used in decision processes without release of the underlying data.
- Assessment of how using artificial intelligence for grid optimization affects cybersecurity (e.g., employee personally identifiable information, Payment Card Industry requirements, information technology/operational technology convergence)
- Framework/approach for quantifying the combined risk of new stakeholders such as smart grid application developers, distributed energy resources, and distributed energy resources aggregation
- Cyber supply chain vulnerability analysis
- Quantification of interrelated risks (e.g., if one stakeholder loses access when another stakeholder is hit by a cyber-related incident).

Challenge: The current standard for contingency planning (to ensure a system has sufficient resources after the loss of a single major unit) is insufficient to quantify indirect consequences that increase with the duration of a power outage.

What is at stake? The consequences of long-duration outages are significantly greater than those of short, local disruptions. Despite the infrequency of these disruptions, characterizing the contingency scenarios that can cause these enduring disruptions is critical to quantify the overall system risk.

Needs in this area include the following:

- Better capabilities for fragility modeling and validation of those models
- A framework for deciding how responsibility should be divided among stakeholders (the responsibility for individual disruptions may rest with different stakeholders)
- Multi-objective co-optimization problem-solving—a method to balance multiple societal/community needs (e.g., Should we prioritize hospitals or military installations?)
- A framework for customer prioritization based on the event and duration of the outage (e.g., Do we need to focus on power or water restoration?)
- Quantification of recovery times (e.g., When will generation and transmission come back online after a hurricane or other disruptive event?).

Challenge: Ensuring equity and protecting vulnerable populations remain challenging.

What is at stake? Fairness in the benefits of the power system helps sustain the public resource model in which customers are willing to cross-fund the development of the grid. This public-mindedness is at the heart of the utility financing model, regardless of whether a municipal or investor-owned entity distributes the costs. Risks can impose additional burden on those who have finite personal resilience resources such as savings and personal transportation access.

Needs in this area include the following:

- Modeling of social and nonmonetary costs (e.g., mortality and morbidity)
- A more holistic framework for utilities to manage the costs of resilience investments for disadvantaged communities
- More data on where vulnerable populations are (in addition to behind the meter/value of load data)
- Census data to include socioeconomic data in risk prioritization processes
- Higher-resolution data on those impacted and making sure these data are incorporated in the ways we project and show results
- Better demographic data for modeling and future projections regarding threat characterization: Who are the people living in a particular area? How many are there? Where are they located?
- Framework for considering the broader implications of long-duration outages on the supply chain of necessities for vulnerable populations
- Framework for quantifying the qualities and necessities of different loads to integrate into resource planning processes
- A prioritization approach to determine critical loads
- More efficient public input/feedback mechanism to include vulnerable populations and sentiment analysis (i.e., public perceptions and acceptability of emerging technologies)
- More stakeholders active in the process (e.g., consumer advocates, community members, governments, and nonprofits)
- More analysis and rigor to demonstrate how everyone benefits from resilience/risk mitigation investments.

Challenge: A lack of use cases harms laypersons' understanding of the value of risk quantification and inhibits optimal decision-making.

What is at stake? Without nuanced understanding of the barriers to risk management, the full capability of a risk quantification initiative cannot be realized. The results must be customized to ensure they meet the need.

Needs in this area include the following:

- Use cases at various scales—local, state, regional, and national—risk may appear and impact markets and long-term planning differently
- Use cases for different electrical systems (e.g., vertically integrated utilities vs. utilities operating in a more deregulated/unstructured environment)
- Integration of trends into the future, such as growing numbers of prosumers or defections from the grid

- Integration of technical issues *and* public policy (e.g., federal policy).

4 Partnerships and Resources

Participants also identified stakeholders and resources to draw on as research into risk quantification progresses. Many of the stakeholders have investments in energy security and resilience and could serve as key participants in future workshops and ongoing dialogue. These stakeholders included insurance companies and investors, developers and builders, owners and operators, state public utility commissioners and staff, state energy offices, federal policymakers and regulators, global supply chain stakeholders, members of the emergency management community, and the defense sector.

Participants also identified stakeholders they saw as having skills, resources, or capabilities that might be leveraged to mitigate some of the challenges discussed. The entities identified on this list included research institutions and agencies, banks, nongovernment organizations and nonprofit organizations, service providers, and national laboratories. The specific energy security and resilience challenges that these entities are particularly suited to address, however, remained outside the scope of this conversation. A select list of such potential partners and resources is included in Figure 3.

Data

- National Oceanic and Atmospheric Administration (NOAA) data real-time layers
- National Center for Atmospheric Research (NCAR) economic losses per disaster
- U.S. Department of Energy's Eagle-I$^{\text{TM}}$ real-time power outages at the county level
- Electric Disturbance Events (OE417) database
- Homeland Infrastructure Foundation-Level Data (HIFLD)
- U.S. Department of Health and Human Services (HHS) power map (electricity-dependent durable medical and assistive equipment [DME])
- Idaho National Laboratory's (INL's) asset-level data and All Hazards Analysis (AHA)
- U.S. Energy Information Agency (EIA) data
- AT&T's Climate Change Analysis Tool (CCAT) data
- Federal Emergency Management Agency (FEMA) disaster impact data
- National Economic Resilience Data Explorer (NERDE)
- Arizona State University (ASU) SHELDUS$^{\text{TM}}$ hazard dataset
- OASIS data

- **Models and Frameworks**
- STAR model of electricity distribution and transmission modeling
- North American Energy Resilience Model (NAERM)
- Argonne National Laboratory's (ANL's) ClimRR
- Lawrence Berkeley National Laboratory's (LBNL's) Power Reliability Event Simulation Tool (PRESTO)
- Oak Ridge National Laboratory's (ORNL's) building and transportation fragility model
- FEMA's National Threat and Hazard Identification and Risk Assessment (THIRA)

- **Other Partners and Resources**
- U.S. Bureau of Economic Analysis (BEA)
- U.S. Geological Survey (USGS)
- MITRE
- ZestyAI
- Riskfactor.com

Figure 3. Stakeholders and resources to inform risk quantification research

5 Conclusion and Next Steps

In the next decade, the pace of change in the energy system is likely to be unprecedented. As we look toward 2035 and beyond, when the electric grid will provide for an even greater percentage of energy needs to the public than it does today, we must take steps to ensure the future grid is secure and resilient to a complex and dynamic threat environment. The first step is to quantify the risks across the energy domain with attention to confidence and complexity. By reducing blind spots in the risk landscape and focusing on the incentives to address known risks, we can ensure the security and resilience of the future electricity grid in service to the nation. Such a risk quantification effort is extremely difficult, is fraught with uncertainty, and requires expertise across many domains. That makes it particularly suited to collaboration across leading research organizations and with deep partnerships from the stakeholders that will ultimately lead risk-aware investments. Our vision is a power sector that is resilient to all hazards and is more economically competitive because all the players know their responsibilities and have the tools, authorities, and relationships to appropriately consider and reduce risks. The workshop NREL convened with relevant stakeholders and researchers was a first step toward improving risk quantification in the electricity system and achieving this vision.

5.1 Next Steps

The themes raised during this workshop will inform national laboratory efforts related to risk quantification and research areas. DOE and other partners, including national laboratories, state and local governments, and industry leaders, will be engaged through follow-up conversations to chart possible research plans.